

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Naomi GO, et al

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: INFORMATION PROVIDING APPARATUS AND METHOD, INFORMATION PROCESSING APPARATUS AND METHOD, AND PROGRAM STORAGE MEDIUM



REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-070461	March 14, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and  
(B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Gregory J. Maier

Registration No. 25,599

C. Irvin McClelland

Registration Number 21,124



22850

5008650500

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年 3月14日

出 願 番 号  
Application Number:

特願2000-070461

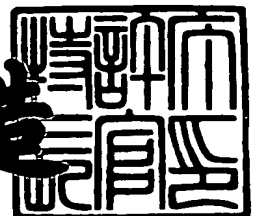
出 願 人  
Applicant(s):

ソニー株式会社

2000年12月22日

特 許 庁 長 官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3106146

【書類名】 特許願

【整理番号】 0000130306

【提出日】 平成12年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
    内

    【氏名】 郷 直美

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
    内

    【氏名】 栗原 章

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100082131

    【弁理士】

    【氏名又は名称】 稲本 義雄

    【電話番号】 03-3369-6479

【手数料の表示】

    【予納台帳番号】 032089

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

特 2 0 0 0 - 0 7 0 4 6 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体

【特許請求の範囲】

【請求項 1】 第 1 の情報処理装置を認証する第 1 の認証手段と、  
第 2 の情報処理装置または第 3 の情報処理装置を認証する第 2 の認証手段と、  
前記第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第 2 の情報処理装置を特定するデータまたは前記第 3 の情報処理装置を特定するデータの受信を制御する受信制御手段と、

前記第 2 の情報処理装置を特定する前記データを受信した場合、前記第 2 の情報処理装置に対応した手順で、前記第 2 の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第 2 の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第 3 の情報処理装置を特定する前記データを受信した場合、前記第 3 の情報処理装置に対応した手順で、前記第 3 の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第 3 の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御手段と、

前記第 1 の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御手段と

を含むことを特徴とする情報提供装置。

【請求項 2】 前記コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段  
を更に含むことを特徴とする請求項 1 に記載の情報提供装置。

【請求項 3】 第 1 の情報処理装置を認証する第 1 の認証ステップと、  
第 2 の情報処理装置または第 3 の情報処理装置を認証する第 2 の認証ステップと、

前記第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第 2 の情報処理装置を特定するデータまたは前記第 3 の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第2の情報処理装置を特定する前記データを受信した場合、前記第2の情報処理装置に対応した手順で、前記第2の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第2の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第3の情報処理装置を特定する前記データを受信した場合、前記第3の情報処理装置に対応した手順で、前記第3の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第3の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第1の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とする情報提供方法。

【請求項4】 第1の情報処理装置を認証する第1の認証ステップと、  
第2の情報処理装置または第3の情報処理装置を認証する第2の認証ステップと、

前記第1の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第2の情報処理装置を特定するデータまたは前記第3の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第2の情報処理装置を特定する前記データを受信した場合、前記第2の情報処理装置に対応した手順で、前記第2の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第2の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第3の情報処理装置を特定する前記データを受信した場合、前記第3の情報処理装置に対応した手順で、前記第3の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第3の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第1の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項 5】 第 1 の情報提供装置を認証する認証手段と、

前記第 1 の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第 2 の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第 3 の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、

前記第 2 の情報提供装置または前記第 3 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御手段と

を含むことを特徴とする情報処理装置。

【請求項 6】 第 1 の情報提供装置を認証する認証ステップと、

前記第 1 の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第 2 の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第 3 の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第 2 の情報提供装置または前記第 3 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 7】 第 1 の情報提供装置を認証する認証ステップと、

前記第 1 の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第 2 の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第 3 の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第 2 の情報提供装置または前記第 3 の情報提供装置から前記第 1 の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

## 【 0 0 0 1 】

## 【発明の属する技術分野】

本発明は、情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、コンテンツおよびコンテンツを復号する鍵を提供するか、または暗号化されているコンテンツを利用する情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関する。

## 【 0 0 0 2 】

## 【従来の技術】

図 1 は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ 1 は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク 4 に接続されている。パーソナルコンピュータ 1 は、コンテンツサーバ 2 2 - 1 若しくは 2 2 - 2 から受信した、または CD (Compact Disc) から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともに DES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

## 【 0 0 0 3 】

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

## 【 0 0 0 4 】

利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス (Portable Device (PDとも称する)) の台数（後述する、いわゆるチェックアウトできる PD の台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ 1 は、そのコンテンツを再生できる。

## 【 0 0 0 5 】

パーソナルコンピュータ 1 の表示操作指示プログラム 1 1 は、パーソナルコンピュータ 1 が記録しているコンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、チェックアウトの指示などを入力して、SDMI (Secure Digital Music Initiative) の規格に準拠したソフトウェア



モジュールである LCM (Licensed Compliant Module) 12 にその指示に対応したチェックアウトなどの処理を実行させる。

【0006】

パーソナルコンピュータ1の LCM12 は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【0007】

LCM12 は、パーソナルコンピュータ1に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、LCM12 は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【0008】

また、LCM12 は、装着されているポータブルメディア3の正当性をチェックして、サーバ5が指定した利用条件をコンテンツ（暗号化されている）に付加して、コンテンツを記録させる。

【0009】

パーソナルコンピュータ1の LCM12 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、接続されているポータブルデバイス2に供給するとともに、ポータブルデバイス2に供給したことに対応して、供給したコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0010】

ポータブルデバイス2は、パーソナルコンピュータ1から供給されたコンテン

ツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、装着されているポータブルメディア3に記憶させる。

【 0 0 1 1 】

ポータブルメディア3は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス2に着脱可能に構成されている。

【 0 0 1 2 】

ポータブルデバイス2は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア3に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【 0 0 1 3 】

例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス2は、対応するコンテンツの再生を停止する。

【 0 0 1 4 】

使用者は、コンテンツを記憶したポータブルデバイス2をパーソナルコンピュータ1から取り外して、持ち歩き、ポータブルメディア3に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【 0 0 1 5 】

ポータブルデバイス2がUSBケーブル等を介してパーソナルコンピュータ1に接続されたとき、ポータブルデバイス2とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ1が生成するある値（チャレンジ）に対して、ポータブルデバイス2がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。

【 0 0 1 6 】

サーバ5-1は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄

積して、パーソナルコンピュータ1からの要求に対応して蓄積しているコンテンツを配信する。サーバ5-1は、鍵サーバ21-1、コンテンツサーバ22-1、およびショップサーバ23-1の機能を有する。

## 【0017】

鍵サーバ21-1は、コンテンツサーバ22-1がパーソナルコンピュータ1に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ1の要求に対応して、コンテンツ鍵をパーソナルコンピュータ1に供給する。コンテンツ鍵の供給の前に、鍵サーバ21-1とパーソナルコンピュータ1とは、相互認証の処理を実行して、鍵サーバ21-1は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ1に送信する。パーソナルコンピュータ1は、受信したコンテンツ鍵を共有している一時鍵で復号する。

## 【0018】

コンテンツサーバ22-1は、パーソナルコンピュータ1の要求に対応して、通信ネットワーク4を介して、パーソナルコンピュータ1に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

## 【0019】

ショップサーバ23-1は、コンテンツサーバ22-1が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ1に提供するとともに、パーソナルコンピュータ1からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ22-1のURL (Uniform Resource Locator)、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ21-1のURLなどをパーソナルコンピュータ1に供給する。

## 【0020】

サーバ5-2は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ1からの要求に対応して蓄積しているコンテンツを配信する。サーバ5-2は、鍵サーバ21-2、コンテンツサーバ22-2、およびショップサーバ23-2の機能を有する。

## 【0021】

鍵サーバ21-2は、コンテンツサーバ22-2がパーソナルコンピュータ1に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ1の要求に対応して、コンテンツ鍵をパーソナルコンピュータ1に供給する。コンテンツ鍵の供給の前に、鍵サーバ21-2とパーソナルコンピュータ1とは、相互認証の処理を実行して、鍵サーバ21-2は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ1に送信する。パーソナルコンピュータ1は、受信したコンテンツ鍵を共有している一時鍵で復号する。

## 【0022】

コンテンツサーバ22-2は、パーソナルコンピュータ1の要求に対応して、通信ネットワーク4を介して、パーソナルコンピュータ1に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

## 【0023】

ショップサーバ23-2は、コンテンツサーバ22-2が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ1に提供するとともに、パーソナルコンピュータ1からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ22-2のURL、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ21-2のURLなどをパーソナルコンピュータ1に供給する。

## 【0024】

以下、サーバ5-1およびサーバ5-2を個々に区別する必要がないとき、単に、サーバ5と称する。以下、鍵サーバ21-1および鍵サーバ21-2を個々に区別する必要がないとき、単に、鍵サーバ21と称する。以下、コンテンツサーバ22-1およびコンテンツサーバ22-2を個々に区別する必要がないとき、単に、コンテンツサーバ22と称する。以下、ショップサーバ23-1およびショップサーバ23-2を個々に区別する必要がないとき、単に、ショップサーバ23と称する。

## 【0025】

次に、図2を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ1は、表示操作指示プログラム11およびLCM12に加えて、IP (Internet Protocol) 通信プログラム13、ISP (Internet Service Provider) 接続プログラム14、およびPHS (Personal Handyphone System) / IMT (International Mobile Telecommunication System) 通信プログラム15を実行する。

## 【0026】

PHS/IMT通信プログラム15は、公衆回線網31を介して通信を行うためのプログラムである。ISP接続プログラム14は、ISP32と接続するためのプログラムである。IP通信プログラム13は、HTTP (Hypertext Transport Protocol) 74およびWap (Wireless Access Protocol) 75などの手続を包含し、通信ネットワーク4を介して、鍵サーバ21、コンテンツサーバ22、またはショップサーバ23と通信するためのプログラムである。

## 【0027】

LCM12は、ライセンス管理プログラム51、ダウンロードプログラム52-1、ダウンロードプログラム52-2、およびフォーマット管理プログラム53から構成されている。

## 【0028】

ライセンス管理プログラム51は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム61、CDリッピングプログラム62、およびPD認証プログラム63から構成されている。

## 【0029】

利用条件管理プログラム61は、コンテンツの利用条件に基づいて、パーソナルコンピュータ1が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリッピングプログラム62は、パーソナルコンピュータ1に装着されたCDからコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

## 【 0 0 3 0 】

PD認証プログラム63は、パーソナルコンピュータ1に装着されているポータブルデバイス2を認証する。

## 【 0 0 3 1 】

ダウンロードプログラム52-1は、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、鍵管理プログラム64、コンテンツ管理プログラム65、鍵情報受信プログラム66、およびコンテンツ情報受信プログラム67から構成されている。

## 【 0 0 3 2 】

鍵管理プログラム64は、鍵サーバ21-1の認証の処理を実行して、鍵サーバ21-1からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム64は、サーバ認証プログラム71および受信プログラム72から構成される。

## 【 0 0 3 3 】

サーバ認証プログラム71は、後述する処理により、鍵サーバ21-1を認証する。受信プログラム72は、通信ネットワーク4を介して、鍵サーバ21-1からコンテンツ鍵を受信する。

## 【 0 0 3 4 】

コンテンツ管理プログラム65は、通信ネットワーク4を介して、コンテンツサーバ22-1からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム65の受信プログラム73は、コンテンツサーバ22-1からコンテンツの利用条件のデータおよびコンテンツを受信する。

## 【 0 0 3 5 】

鍵情報受信プログラム66は、ショップサーバ23-1から、所望のコンテンツに対応するコンテンツ鍵を供給する鍵サーバ21-1を特定するURLを受信する。コンテンツ情報受信プログラム67は、ショップサーバ23-1から、使用者が所望するコンテンツを特定するコンテンツID、およびそのコンテンツを供給するコンテンツサーバ22-1を特定するURLを受信する。

【0036】

ダウンロードプログラム52-2は、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、ダウンロードプログラム52-1と同様の構成を有するので、その説明は省略する。

【0037】

フォーマット管理プログラム53は、コンテンツサーバ22-1または22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換するとともに、CDから読み出したコンテンツを所定の方式で符号化して暗号化する。フォーマット管理プログラム53は、システム識別プログラム68およびフォーマット変換プログラム69から構成されている。

【0038】

システム識別プログラム68は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム69は、コンテンツの符号化方式および暗号化方式を変換する。

【0039】

ポータブルデバイス2は、ライセンス管理プログラム81、鍵管理プログラム82、およびコンテンツ管理プログラム83を実行する。

【0040】

ライセンス管理プログラム81は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム91、パーソナルコンピュータ1を認証するPC認証プログラム92、およびポータブルメディア3を認証するPM認証プログラム93から構成される。

【0041】

鍵管理プログラム82は、パーソナルコンピュータ1から供給されたコンテンツ鍵を、ポータブルメディア3が予め記憶している保存用鍵で暗号化させ、ポータブルメディア3に記憶させて管理する。

【0042】

コンテンツ管理プログラム83は、パーソナルコンピュータ1から供給された

コンテンツを、ポータブルメディア3に記憶させて管理する。

【0043】

ポータブルメディア3は、ライセンス管理プログラム101、鍵管理プログラム102、およびコンテンツ管理プログラム103を実行する。

【0044】

ライセンス管理プログラム101は、ポータブルデバイス2を認証するPD認証プログラム111を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム102は、ポータブルデバイス2から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コンテンツ管理プログラム103は、ポータブルデバイス2から供給されたコンテンツを記憶して、管理する。

【0045】

ショップサーバ23-1は、鍵情報送信プログラム121、コンテンツ情報送信プログラム122、閲覧プログラム123、およびIP通信プログラム124を実行する。

【0046】

鍵情報送信プログラム121は、通信ネットワーク4を介して、パーソナルコンピュータ1に、パーソナルコンピュータ1の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ21-1のURLを送信する。

【0047】

コンテンツ情報送信プログラム122は、通信ネットワーク4を介して、パーソナルコンピュータ1に、パーソナルコンピュータ1の使用者が所望するコンテンツを供給するコンテンツサーバ22-1のURLを送信する。

【0048】

閲覧プログラム123は、コンテンツをパーソナルコンピュータ1の使用者に視聴させる視聴プログラム131、およびパーソナルコンピュータ1の使用者が所望のコンテンツを検索する検索プログラム132から構成されている。

【0049】



IP通信プログラム124は、HTTP133およびWap134などの手続を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1と通信するためのプログラムである。

【0050】

鍵サーバ21-1は、認証プログラム151、鍵配信プログラム152、鍵保存プログラム153、鍵生成プログラム154、およびIP通信プログラム155を実行する。

【0051】

認証プログラム151は、パーソナルコンピュータ1などを認証するプログラムである。鍵配信プログラム152は、認証されたパーソナルコンピュータ1に、鍵保存プログラム153が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム153は、鍵生成プログラム154により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム154は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【0052】

IP通信プログラム155は、HTTP171およびWap172などの手続を包含し、通信ネットワーク4を介して、パーソナルコンピュータ1などと通信するためのプログラムである。

【0053】

コンテンツサーバ22-1は、コンテンツ保存プログラム191、コンテンツ配信プログラム192、およびIP通信プログラム193を実行する。

【0054】

コンテンツ保存プログラム191は、暗号化されているコンテンツをコンテンツIDと対応させて保存する。コンテンツ配信プログラム192は、パーソナルコンピュータ1から要求があったとき、コンテンツ保存プログラム191が保存している、コンテンツIDに対応するコンテンツをパーソナルコンピュータ1に配信する。

【0055】

IP通信プログラム193は、HTTP201およびWap202などの手続

を包含し、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 と通信するためのプログラムである。

【 0 0 5 6 】

ショップサーバ 2 3 - 2 は、ショップサーバ 2 3 - 1 と同様の構成を有するので、その説明は省略する。鍵サーバ 2 1 - 2 は、鍵サーバ 2 1 - 1 と同様の構成を有するので、その説明は省略する。コンテンツサーバ 2 2 - 2 は、コンテンツサーバ 2 2 - 1 と同様の構成を有するのでその説明は省略する。

【 0 0 5 7 】

次に、パーソナルコンピュータ 1 がサーバ 5 - 1 からコンテンツをダウンロードして、ポータブルデバイス 2 にチェックアウトする従来の処理を図 3 および図 4 のフローチャートを参照して説明する。ステップ S 1 0 1 において、パーソナルコンピュータ 1 の P H S / I M T 通信プログラム 1 5 は、公衆回線網 3 1 と接続を確立する。ステップ S 2 0 1 において、公衆回線網 3 1 の図示せぬ地上局などは、パーソナルコンピュータ 1 と接続を確立する。

【 0 0 5 8 】

ステップ S 1 0 2 において、パーソナルコンピュータ 1 の I S P 接続プログラム 1 4 は、I S P 3 2 と接続を確立する。ステップ S 3 0 1 において、I S P 3 2 は、パーソナルコンピュータ 1 と接続を確立する。

【 0 0 5 9 】

ステップ S 1 0 3 において、パーソナルコンピュータ 1 の I P 通信プログラム 1 3 は、ショップサーバ 2 3 と I P 通信を確立する。ステップ S 4 0 1 において、ショップサーバ 2 3 - 1 の I P 通信プログラム 1 2 4 は、パーソナルコンピュータ 1 と I P 通信を確立する。

【 0 0 6 0 】

ステップ S 4 0 2 において、ショップサーバ 2 3 - 1 の閲覧プログラム 1 2 3 は、通信ネットワーク 4 を介して、パーソナルコンピュータ 1 に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップ S 1 0 4 において、パーソナルコンピュータ 1 の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナル

コンピュータ 1 のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ 2 3 - 1 の閲覧プログラム 1 2 3 に検索させ、その結果を表示する。ステップ S 4 0 2 およびステップ S 1 0 4 の処理は、パーソナルコンピュータ 1 の使用者の要求に対応して、繰り返される。

## 【 0 0 6 1 】

ステップ S 1 0 5 において、パーソナルコンピュータ 1 のブラウザプログラムは、購入依頼をショップサーバ 2 3 - 1 に送信する。ステップ S 4 0 3 において、ショップサーバ 2 3 - 1 の閲覧プログラム 1 2 3 は、パーソナルコンピュータ 1 から送信された購入依頼を受信する。

## 【 0 0 6 2 】

ステップ S 4 0 4 において、ショップサーバ 2 3 - 1 のコンテンツ情報送信プログラム 1 2 2 は、ステップ S 4 0 3 の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ 2 2 - 1 の URL およびコンテンツを特定するためのコンテンツ ID などを含む、コンテンツ情報を通信ネットワーク 4 を介してパーソナルコンピュータ 1 に送信する。ステップ S 1 0 6 において、パーソナルコンピュータ 1 のコンテンツ情報受信プログラム 6 7 は、ショップサーバ 2 3 - 1 が送信した、コンテンツ情報を受信する。

## 【 0 0 6 3 】

ステップ S 4 0 5 において、ショップサーバ 2 3 - 1 の鍵情報送信プログラム 1 2 1 は、ステップ S 4 0 3 の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ 2 1 - 1 の URL などの、鍵情報を通信ネットワーク 4 を介してパーソナルコンピュータ 1 に送信する。ステップ S 1 0 7 において、パーソナルコンピュータ 1 の鍵情報受信プログラム 6 6 は、ショップサーバ 2 3 - 1 が送信した鍵情報を受信する。

## 【 0 0 6 4 】

ステップ S 1 0 8 において、パーソナルコンピュータ 1 の IP 通信プログラム 1 3 は、ステップ S 1 0 6 の処理で取得したコンテンツ情報に含まれるコンテンツサーバ 2 2 - 1 の URL を基に、コンテンツサーバ 2 2 - 1 と IP 通信を確立

する。ステップS501において、コンテンツサーバ22-1のIP通信プログラム193は、パーソナルコンピュータ1とIP通信を確立する。

## 【0065】

ステップS109において、パーソナルコンピュータ1のコンテンツ管理プログラム65は、ステップS106の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-1に送信する。ステップS502において、コンテンツサーバ22-1は、パーソナルコンピュータ1が送信したコンテンツIDを受信する。ステップS503において、コンテンツサーバ22-1のコンテンツ配信プログラム192は、ステップS502で受信したコンテンツIDに対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム191から読み出して、通信ネットワーク4を介して、パーソナルコンピュータ1に配信する。ステップS110において、パーソナルコンピュータ1のコンテンツ管理プログラム65の受信プログラム73は、コンテンツサーバ22-1が送信したコンテンツを受信する。

## 【0066】

ステップS111において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS107の処理で取得した鍵情報に含まれる鍵サーバ21-1のURLを基に、鍵サーバ21-1とIP通信を確立する。ステップS601において、鍵サーバ21-1のIP通信プログラム155は、パーソナルコンピュータ1とIP通信を確立する。

## 【0067】

ステップS112において、パーソナルコンピュータ1の鍵管理プログラム64のサーバ認証プログラム71は、鍵サーバ21-1を認証する。ステップS602において、鍵サーバ21-1の認証プログラム151は、パーソナルコンピュータ1を認証する。

## 【0068】

鍵サーバ21-1には、マスター鍵KMSが予め記憶されており、パーソナルコンピュータ1には、個別鍵KPPとパーソナルコンピュータ1のIDが予め記憶されている。パーソナルコンピュータ1には、更に、マスター鍵KMPが予め記憶され

ており、鍵サーバ21-1にも鍵サーバ21-1のIDと個別鍵KPSが記憶されている。

【0069】

鍵サーバ21-1は、パーソナルコンピュータ1から、パーソナルコンピュータ1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSにハッシュ関数を適用して、パーソナルコンピュータ1の個別鍵KPPと同一の鍵を生成する。

【0070】

パーソナルコンピュータ1は、鍵サーバ21-1から、鍵サーバ21-1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMPにハッシュ関数を適用して、鍵サーバ21-1の個別鍵KPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1と鍵サーバ21-1の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

【0071】

ステップS113において、パーソナルコンピュータ1の鍵管理プログラム64は、コンテンツIDを鍵サーバ21-1に送信する。ステップS603において、鍵サーバ21-1は、パーソナルコンピュータ1が送信した、コンテンツIDを受信する。ステップS604において、鍵サーバ21-1の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ1に送信する。ステップS114において、パーソナルコンピュータ1の鍵管理プログラム64の受信プログラム72は、鍵サーバ21-1が送信したコンテンツ鍵を受信する。鍵管理プログラム64は、受信したコンテンツ鍵を一時鍵で復号する。

【0072】

ステップS115において、パーソナルコンピュータ1のPHS/IMT通信プログラム15は、公衆回線網31との接続を切断する。ステップS202において、公衆回線網31の図示せぬ地上局などは、パーソナルコンピュータ1との接続を切断する。

【0073】

ステップS116において、フォーマット管理プログラム53は、ステップS110の処理で受信したコンテンツの符号化方式および暗号化方式を、それぞれ所定の方式に変換する。

【0074】

パーソナルコンピュータ1の使用者が、表示操作指示プログラム11に対し、受信したコンテンツのチェックアウトを指示したとき、ステップS117以降の処理が実行される。

【0075】

ステップS117において、パーソナルコンピュータ1のライセンス管理プログラム51のPD認証プログラム63は、ポータブルデバイス2を認証する。ステップS701において、ポータブルデバイス2のライセンス管理プログラム81のPC認証プログラム92は、パーソナルコンピュータ1を認証する。

【0076】

ステップS117およびステップS701におけるパーソナルコンピュータ1とポータブルデバイス2との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップS112およびステップS602における鍵サーバ21-1とパーソナルコンピュータ1との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ1およびポータブルデバイス2は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【0077】

ステップS118において、パーソナルコンピュータ1のコンテンツ管理プログラム65は、暗号化されているコンテンツをポータブルデバイス2に配信する。ステップS702において、ポータブルデバイス2のコンテンツ管理プログラム83は、パーソナルコンピュータ1が配信したコンテンツを受信して、ポータブルメディア3のコンテンツ管理プログラム103に供給する。ポータブルメディア3のコンテンツ管理プログラム103は、コンテンツを記憶する。

【0078】

なお、ポータブルデバイス2とポータブルメディア3は、ポータブルデバイス2にポータブルメディア3が装着されたとき、相互認証する。

## 【0079】

ステップS119において、パーソナルコンピュータ1の鍵管理プログラム64は、ポータブルデバイス2に、ステップS118で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス2とポータブルメディア3とで共有する一時鍵で暗号化されている）を配信する。ステップS703において、ポータブルデバイス2の鍵管理プログラム82は、パーソナルコンピュータ1が配信したコンテンツ鍵を受信して、ポータブルメディア3の鍵管理プログラム102に供給する。ポータブルメディア3の鍵管理プログラム102は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

## 【0080】

次に、パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする処理を図5および図6のフローチャートを参照して説明する。ステップS1101乃至ステップS1107の処理は、サーバ5-2、並びにIP通信プログラム13、ISP接続プログラム14、PHS/IMT通信プログラム15、およびダウンロードプログラム52-2により実行され、それぞれ、ステップS101乃至ステップS107の処理と同様なので、その説明は省略する。

## 【0081】

ステップS1108において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS1107の処理で取得した鍵情報に含まれる鍵サーバ21-2のURLを基に、鍵サーバ21-2とIP通信を確立する。ステップS1601において、鍵サーバ21-2は、パーソナルコンピュータ1とIP通信を確立する。

## 【0082】

ステップS1109において、パーソナルコンピュータ1のダウンロードプログラム52-2は、鍵サーバ21-2を認証する。ステップS1602において、鍵サーバ21-2は、パーソナルコンピュータ1を認証する。ステップS1109およびステップS1602の処理は、ステップS112およびステップS602の処理と同様の処理である。

## 【0083】

ステップS1110において、パーソナルコンピュータ1のダウンロードプログラム52-2は、コンテンツIDを鍵サーバ21-2に送信する。ステップS1603において、鍵サーバ21-2は、パーソナルコンピュータ1が送信した、コンテンツIDを受信する。ステップS1604において、鍵サーバ21-2は、コンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ1に送信する。ステップS1111において、パーソナルコンピュータ1のダウンロードプログラム52-2は、鍵サーバ21-2が送信したコンテンツ鍵を受信する。ダウンロードプログラム52-2は、受信したコンテンツ鍵を一時鍵で復号する。

## 【0084】

ステップS1112において、パーソナルコンピュータ1のIP通信プログラム13は、ステップS1106の処理で取得したコンテンツ情報に含まれるコンテンツサーバ22-2のURLを基に、コンテンツサーバ22-2とIP通信を確立する。ステップS1501において、コンテンツサーバ22-2は、パーソナルコンピュータ1とIP通信を確立する。

## 【0085】

ステップS1113において、パーソナルコンピュータ1のダウンロードプログラム52-2は、ステップS1106の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-2に送信する。ステップS1502において、コンテンツサーバ22-2は、パーソナルコンピュータ1が送信したコンテンツIDを受信する。ステップS1503において、コンテンツサーバ22-2は、ステップS1502で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク4を介して、パーソナルコンピュータ1に配信する。ステップS1114において、パーソナルコンピュータ1のダウンロードプログラム52-2は、コンテンツサーバ22-2が送信したコンテンツを受信する。

## 【0086】



ステップ S 1 1 1 5 乃至ステップ S 1 7 0 3 の処理は、ステップ S 1 1 5 乃至ステップ S 7 0 3 の処理と同様なので、その説明は省略する。

【 0 0 8 7 】

【発明が解決しようとする課題】

以上のように、コンテンツおよびコンテンツ鍵を供給するサーバ 5 - 1 または 5 - 2 は、それぞれ、コンテンツおよびコンテンツ鍵を供給する手順が異なるので、サーバ 5 - 1 および 5 - 2 からのコンテンツの受信を所望する場合、サーバ 5 - 1 に対応するダウンロードプログラム 5 2 - 1 とサーバ 5 - 2 に対応するダウンロードプログラム 5 2 - 2 とが必要となる。

【 0 0 8 8 】

しかしながら、コンテンツを受信する装置の、演算能力が小さい、記憶容量が少ないなどの処理能力が小さい場合、コンテンツを受信する装置は、複数のダウンロードプログラムを記憶しておくことができず、ダウンロードプログラムを切り換えて実行することができない。

【 0 0 8 9 】

本発明はこのような状況に鑑みてなされたものであり、処理能力が小さい装置でも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようにすることを目的とする。

【 0 0 9 0 】

【課題を解決するための手段】

請求項 1 に記載の情報提供装置は、第 1 の情報処理装置を認証する第 1 の認証手段と、第 2 の情報処理装置または第 3 の情報処理装置を認証する第 2 の認証手段と、第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第 2 の情報処理装置を特定するデータまたは第 3 の情報処理装置を特定するデータの受信を制御する受信制御手段と、第 2 の情報処理装置を特定するデータを受信した場合、第 2 の情報処理装置に対応した手順で、第 2 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 2 の情報処理装置からコンテンツおよび鍵を受信し、第 3 の情報処理装置を特定するデータを受信した場合、第 3 の情報処理装置に対応した手順で、第 3 の情報処理装置にコンテンツおよび鍵の

送信要求を送信するとともに、第 3 の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御手段と、第 1 の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御手段とを含むことを特徴とする。

## 【 0 0 9 1 】

情報提供装置は、コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に設けることができる。

## 【 0 0 9 2 】

請求項 3 に記載の情報提供方法は、第 1 の情報処理装置を認証する第 1 の認証ステップと、第 2 の情報処理装置または第 3 の情報処理装置を認証する第 2 の認証ステップと、第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第 2 の情報処理装置を特定するデータまたは第 3 の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第 2 の情報処理装置を特定するデータを受信した場合、第 2 の情報処理装置に対応した手順で、第 2 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 2 の情報処理装置からコンテンツおよび鍵を受信し、第 3 の情報処理装置を特定するデータを受信した場合、第 3 の情報処理装置に対応した手順で、第 3 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 3 の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第 1 の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

## 【 0 0 9 3 】

請求項 4 に記載のプログラム格納媒体のプログラムは、第 1 の情報処理装置を認証する第 1 の認証ステップと、第 2 の情報処理装置または第 3 の情報処理装置を認証する第 2 の認証ステップと、第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第 2 の情報処理装置を特定するデータまたは第 3 の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第 2 の情報処理装置を特定するデータを受信した場合、第 2 の情報処理装置に対応した手順で、第 2 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第

2の情報処理装置からコンテンツおよび鍵を受信し、第3の情報処理装置を特定するデータを受信した場合、第3の情報処理装置に対応した手順で、第3の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第3の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第1の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

## 【 0 0 9 4 】

請求項5に記載の情報処理装置は、第1の情報提供装置を認証する認証手段と、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御手段とを含むことを特徴とする。

## 【 0 0 9 5 】

請求項6に記載の情報処理方法は、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

## 【 0 0 9 6 】

請求項7に記載のプログラム格納媒体のプログラムは、第1の情報提供装置を認証する認証ステップと、第1の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第2の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第3の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第2の情報提供装置または第3の情報提供装置から第1の情報提供装置が提供を受け、送信したコンテンツお

よび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【 0 0 9 7 】

請求項 1 に記載の情報提供装置、請求項 3 に記載の情報提供方法、および請求項 4 に記載のプログラム格納媒体においては、第 1 の情報処理装置が認証され、第 2 の情報処理装置または第 3 の情報処理装置が認証され、第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第 2 の情報処理装置を特定するデータまたは第 3 の情報処理装置を特定するデータの受信が制御され、第 2 の情報処理装置を特定するデータを受信した場合、第 2 の情報処理装置に対応した手順で、第 2 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 2 の情報処理装置からコンテンツおよび鍵を受信し、第 3 の情報処理装置を特定するデータを受信した場合、第 3 の情報処理装置に対応した手順で、第 3 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 3 の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第 1 の情報処理装置へのコンテンツおよび鍵の送信が制御される。

【 0 0 9 8 】

請求項 5 に記載の情報処理装置、請求項 6 に記載の情報処理方法、および請求項 7 に記載のプログラム格納媒体においては、第 1 の情報提供装置が認証され、第 1 の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第 2 の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第 3 の情報提供装置を特定するデータのいずれかの送信が制御され、第 2 の情報提供装置または第 3 の情報提供装置から第 1 の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御される。

【 0 0 9 9 】

【発明の実施の形態】

図 7 は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図 1 で説明した構成の場合と同一の部分には、図 1 の場合と同一の番号を付してあり、その説明は省略する。

【 0 1 0 0 】

電話機一体型端末機 5 0 1 は、ポータブルメディア 3 - 1 が装着可能に構成さ

れ、無線により、通信ネットワーク 4 に接続される。電話機一体型端末機 5 0 1 は、通信ネットワーク 4 を介して、コンテンツサーバ 2 2 - 1 または 2 2 - 2 から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件データを装着されているポータブルメディア 3 - 1 に記憶させる。

## 【 0 1 0 1 】

電話機一体型端末機 5 0 1 は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア 3 - 1 に記憶されているコンテンツを再生し、図示せぬヘッドフォンまたはスピーカなどに出力する。使用者は、電話機一体型端末機 5 0 1 を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア 3 - 1 に記憶させることができる。使用者は、電話機一体型端末機 5 0 1 に、ポータブルメディア 3 - 1 に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

## 【 0 1 0 2 】

電話機一体型端末機 5 0 1 の表示操作指示プログラム 5 1 1 は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロードの指示などを入力して、クライアント用 LCM 5 1 2 にその指示に対応した処理を実行させる。電話機一体型端末機 5 0 1 のクライアント用 LCM 5 1 2 は、代理サーバ 5 0 3 のサーバ用 LCM 5 1 4 と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

## 【 0 1 0 3 】

電話機一体型端末機 5 0 1 のクライアント用 LCM 5 1 2 は、コンテンツの不正な 2 次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

## 【 0 1 0 4 】

クライアント用 LCM 5 1 2 は、電話機一体型端末機 5 0 1 に装着されている

ポータブルメディア3-1が正当であるかの認証を行い、安全な方法でサーバ5が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア3-1にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用LCM512は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア3-1との通信を制御する。

## 【0105】

パーソナルコンピュータ502は、通信ネットワーク4に接続されている。パーソナルコンピュータ502は、コンテンツサーバ22-1若しくは22-2から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗号化方式で暗号化して記録する。パーソナルコンピュータ502は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

## 【0106】

パーソナルコンピュータ502の表示操作指示プログラム11は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、LCM513にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させる。

## 【0107】

パーソナルコンピュータ502のLCM513は、コンテンツの不正な2次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

## 【0108】

LCM513は、パーソナルコンピュータ502に接続されたポータブルデバイス2が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、LCM513は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との

通信を制御する。

【0109】

また、LCM513は、ポータブルデバイス2の正当性をチェックする。ポータブルデバイス2は、ポータブルメディア3-2が装着されたとき、ポータブルメディア3-2の正当性をチェックする。ポータブルデバイス2およびポータブルメディア3-2が正当である場合、LCM513は、サーバ5が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア3-2にコンテンツをチェックアウトする。ポータブルデバイス2は、パーソナルコンピュータ502からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア3-2に記憶させる。

【0110】

パーソナルコンピュータ502のLCM513は、暗号化して記録しているコンテンツを、接続されているポータブルデバイス2にチェックアウトする。ポータブルデバイス2は、パーソナルコンピュータ502からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア3-2に記憶させる。

【0111】

代理サーバ503を利用できるとき、パーソナルコンピュータ502のPC用LCM521（LCM513の一部または全部の機能から構成される）は、代理サーバ503のサーバ用LCM514と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【0112】

代理サーバ503を利用できないとき、パーソナルコンピュータ502のLCM513は、LCM12と同様の鍵サーバ21-1または21-2との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【0113】

代理サーバ503は、サーバ用LCM514を実行して、相互認証した電話機一体型端末機501または相互認証したパーソナルコンピュータ502の要求に

対応して、鍵サーバ 2 1 - 1 または 2 1 - 2 との認証の処理を実行する。代理サーバ 5 0 3 は、鍵サーバ 2 1 - 1 または 2 1 - 2 との相互認証の処理の後、鍵サーバ 2 1 - 1 または 2 1 - 2 からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 に供給する。代理サーバ 5 0 3 は、コンテンツサーバ 2 2 - 1 または 2 2 - 2 からコンテンツを受信して、受信したコンテンツを電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 に供給する。

## 【 0 1 1 4 】

代理サーバ 5 0 3 は、サーバ 5 - 1 からコンテンツおよびコンテンツ鍵をダウンロードするとき、サーバ 5 - 1 からコンテンツを受信した後、コンテンツ鍵を受信する。代理サーバ 5 0 3 は、サーバ 5 - 2 からコンテンツおよびコンテンツ鍵をダウンロードするとき、コンテンツ鍵を受信した後、コンテンツを受信する。

## 【 0 1 1 5 】

代理サーバ 5 0 3 は、サーバ 5 - 1 からコンテンツおよびコンテンツ鍵をダウンロードしたときも、サーバ 5 - 2 からコンテンツおよびコンテンツ鍵をダウンロードしたときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を送信してから、コンテンツを送信する）で、電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 にコンテンツおよびコンテンツ鍵を供給する。

## 【 0 1 1 6 】

電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 は、代理サーバ 5 0 3 を介して、サーバ 5 - 1 または 5 - 2 からコンテンツおよびコンテンツ鍵をダウンロードすることにより、同一の手順でコンテンツおよびコンテンツ鍵を受信することができる。

## 【 0 1 1 7 】

図 8 は、電話機一体型端末機 5 0 1 の構成を説明する図である。CPU (Central Processing Unit) 6 0 1 は、ROM (Read-only Memory) 6 0 2 または RAM (Random-Access Memory) 6 0 3 に格納されている各種プログラムを実際に実行する。ROM 6 0 2 は、EEPROM (Electrically Erasable Programmable Read-Only Memory



）またはフラッシュメモリなどで構成され、一般的には、CPU 6 0 1 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM 6 0 3 は、SRAM (Static RAM) など構成され、CPU 6 0 1 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

## 【 0 1 1 8 】

入力部 6 0 5 は、入力キーまたはマイクロフォンなどで構成され、CPU 6 0 1 に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部 6 0 6 は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。

## 【 0 1 1 9 】

音声再生部 6 0 7 は、通信部 6 0 8 から供給された通話相手の音声のデータ、またはインターフェース 6 0 9 から供給されたポータブルメディア 3 - 1 に記憶されているコンテンツを再生して、音声を出力する。

## 【 0 1 2 0 】

通信部 6 0 8 は、公衆回線網 3 1 と接続し、CPU 6 0 1 から供給されたデータ（例えば、コンテンツの送信要求など）または入力部 6 0 5 から供給された使用者の音声のデータを、所定の方式のパケットに格納して、公衆回線網 3 1 を介して、送信する。また、通信部 6 0 8 は、公衆回線網 3 1 を介して、受信したパケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU 6 0 1、RAM 6 0 3、音声再生部 6 0 7、またはインターフェース 6 0 9 に出力する。

## 【 0 1 2 1 】

インターフェース 6 0 9 は、CPU 6 0 1、RAM 6 0 3、または通信部 6 0 8 から供給されたデータを装着されているポータブルメディア 3 - 1 に記憶させるとともに、装着されているポータブルメディア 3 - 1 からコンテンツなどのデータを読み出して、CPU 6 0 1、RAM 6 0 3、または音声再生部 6 0 7 に供給する。

## 【 0 1 2 2 】

インターフェース 6 1 0 は、外付けのドライブ 6 3 1 が接続される。ドライブ 6 3 1 は、装着されている磁気ディスク 6 4 1、光ディスク 6 4 2（CD-ROMを含

む)、光磁気ディスク643、または半導体メモリ644に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース610、およびバス604を介して接続されているROM602またはRAM603に供給する。

#### 【0123】

CPU601乃至インターフェース610は、バス604により相互に接続されている。

#### 【0124】

図9は、代理サーバ503の構成を説明する図である。CPU651は、各種アプリケーションプログラム(詳細については後述する)や、OS(Operating System)を実際に実行する。ROM652は、一般的には、CPU651が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM653は、CPU651の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス654により相互に接続されている。

#### 【0125】

ホストバス654は、ブリッジ655を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス656に接続されている。

#### 【0126】

キーボード658は、CPU651に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス659は、ディスプレイ660の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ660は、液晶表示装置またはCRT(Cathode Ray Tube)などから成り、各種情報をテキストやイメージで表示する。HDD(Hard Disk Drive)661は、ハードディスクを駆動し、それらにCPU651によって実行するプログラムや情報を記録または再生させる。

#### 【0127】

ドライブ662は、装着されている磁気ディスク681、光ディスク682、光磁気ディスク683、または半導体メモリ684に記録されているデータまた

はプログラムを読み出して、そのデータまたはプログラムを、インターフェース 657、外部バス 656、ブリッジ 655、およびホストバス 654 を介して接続されている RAM 653 に供給する。

【0128】

これらのキーボード 658 乃至ドライブ 662 は、インターフェース 657 に接続されており、インターフェース 657 は、外部バス 656、ブリッジ 655、およびホストバス 654 を介して CPU 651 に接続されている。

【0129】

通信部 663 は、通信ネットワーク 4 が接続され、CPU 651、または HDD 661 から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のパケットに格納して、通信ネットワーク 4 を介して、送信するとともに、通信ネットワーク 4 を介して、受信したパケットに格納されているデータ（例えば、コンテンツ ID など）を CPU 651、RAM 653、または HDD 661 に出力する。

【0130】

通信部 663 は、外部バス 656、ブリッジ 655、およびホストバス 654 を介して CPU 651 に接続されている。

【0131】

次に、図 10 を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図 2 で説明した構成の場合と同一の部分には、図 2 の場合と同一の番号を付してあり、その説明は省略する。

【0132】

電話機一体型端末機 501 は、表示操作指示プログラム 511、クライアント用 LCM 512、IP 通信プログラム 701、ISP 接続プログラム 702、および PHS/IMT 通信プログラム 703 を実行する。

【0133】

PHS/IMT 通信プログラム 703 は、公衆回線網 31 を介して通信を行うためのプログラムである。ISP 接続プログラム 702 は、ISP 32 と接続するためのプログラムである。IP 通信プログラム 701 は、HTTP 741 および Wap 742 などの手続を包含し、通信ネットワーク 4 を介して、鍵サーバ 2

1-1、コンテンツサーバ22-1、ショップサーバ23-1、鍵サーバ21-2、コンテンツサーバ22-2、ショップサーバ23-2、または代理サーバ503などと通信するためのプログラムである。

【0134】

クライアント用LCM512は、ライセンス管理プログラム711、ダウンロードプログラム712、およびフォーマット管理プログラム713などから構成されている。

【0135】

ライセンス管理プログラム711は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム721、サーバ認証プログラム722、およびPM認証プログラム723などから構成されている。

【0136】

利用条件管理プログラム721は、コンテンツの利用条件に基づいて、ポータブルメディア3-1が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア3-1が記憶しているコンテンツの再生などに対応して、ポータブルメディア3-1に、ポータブルメディア3-1が記憶している利用条件のデータを更新させる。サーバ認証プログラム722は、通信ネットワーク4を介して、代理サーバ503を認証する。PM認証プログラム723は、ポータブルメディア3-1が電話機一体型端末機501に装着されたとき、ポータブルメディア3-1を認証する。

【0137】

ダウンロードプログラム712は、鍵管理プログラム724、コンテンツ管理プログラム725、鍵情報受信プログラム726、およびコンテンツ情報受信プログラム727などから構成されている。

【0138】

鍵管理プログラム724は、代理サーバ503からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア3-1に記憶させて、管理する。鍵管理プログラム724は、代理サーバ503からコンテンツ鍵

を受信する受信プログラム731などを含む。

【0139】

コンテンツ管理プログラム725は、代理サーバ503からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア3-1に記憶させる。コンテンツ管理プログラム725の受信プログラム732は、代理サーバ503からコンテンツの利用条件およびコンテンツを受信する。

【0140】

鍵情報受信プログラム726は、ショップサーバ23-1または23-2から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ21-1または21-2を特定するURLを受信する。コンテンツ情報受信プログラム727は、ショップサーバ23-1または23-2から、所望のコンテンツを特定するコンテンツID、および所望のコンテンツを供給するコンテンツサーバ22-1または22-2を特定するURLを受信する。

【0141】

フォーマット管理プログラム713は、代理サーバ503を介して、コンテンツサーバ22-1または22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム713は、システム識別プログラム728およびフォーマット変換プログラム729などから構成されている。

【0142】

システム識別プログラム728は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム729は、コンテンツの符号化方式および暗号化方式を変換する。

【0143】

次に、代理サーバ503の構成について説明する。代理サーバ503は、サーバ用LCM514、およびIP通信プログラム751を実行する。

【0144】

サーバ用LCM514は、ライセンス管理プログラム761、およびシーケンス管理プログラム762などを含む。

【0145】

ライセンス管理プログラム761は、更に、鍵サーバ21-1または21-2を認証するサーバ認証プログラム781、および電話機一体型端末機501を認証するPD認証プログラム782などを含む。

【0146】

シーケンス管理プログラム762は、鍵管理プログラム771、コンテンツ管理プログラム772、およびシステム識別プログラム773などを含む。

【0147】

鍵管理プログラム771は、更に、通信ネットワーク4を介して、鍵サーバ21-1または21-2からコンテンツ鍵を受信する鍵受信プログラム783、および通信ネットワーク4を介して、受信したコンテンツ鍵を電話機一体型端末機501に配信する鍵配信プログラム784などを含む。

【0148】

コンテンツ管理プログラム772は、更に、通信ネットワーク4を介して、コンテンツサーバ22-1または22-2からコンテンツを受信するコンテンツ受信プログラム785、および通信ネットワーク4を介して、受信したコンテンツを電話機一体型端末機501に配信するコンテンツ配信プログラム786などを含む。

【0149】

システム識別プログラム773は、電話機一体型端末機501から供給されたコンテンツIDを基に、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。

【0150】

IP通信プログラム751は、HTTP787およびWap788などの手続を包含し、通信ネットワーク4を介して、サーバ5-1若しくは5-2、または電話機一体型端末機501と通信するためのプログラムである。

【0151】

次に、電話機一体型端末機 5 0 1 がサーバ 5 - 1 からコンテンツをダウンロードする処理を図 1 1 および図 1 2 のフローチャートを参照して説明する。ステップ S 2 1 0 1 において、電話機一体型端末機 5 0 1 の P H S / I M T 通信プログラム 7 0 3 は、公衆回線網 3 1 と接続を確立する。ステップ S 2 2 0 1 において、公衆回線網 3 1 の図示せぬ地上局などは、電話機一体型端末機 5 0 1 と接続を確立する。

【 0 1 5 2 】

ステップ S 2 1 0 2 において、電話機一体型端末機 5 0 1 の I S P 接続プログラム 7 0 2 は、電話機一体型端末機 5 0 1 と公衆回線網 3 1 との接続を介して、I S P 3 2 と接続を確立する。ステップ S 2 3 0 1 において、I S P 3 2 は、電話機一体型端末機 5 0 1 と公衆回線網 3 1 との接続を介して、電話機一体型端末機 5 0 1 と接続を確立する。

【 0 1 5 3 】

以降の電話機一体型端末機 5 0 1 と、鍵サーバ 2 1 - 1、コンテンツサーバ 2 2 - 1、ショップサーバ 2 3 - 1、または代理サーバ 5 0 3 との処理は、電話機一体型端末機 5 0 1 と I S P 3 2 との接続を介して実行される。

【 0 1 5 4 】

ステップ S 2 1 0 3 において、電話機一体型端末機 5 0 1 の I P 通信プログラム 7 0 1 は、ショップサーバ 2 3 - 1 と I P 通信を確立する。ステップ S 2 4 0 1 において、ショップサーバ 2 3 - 1 の I P 通信プログラム 1 2 4 は、電話機一体型端末機 5 0 1 と I P 通信を確立する。

【 0 1 5 5 】

ステップ S 2 4 0 2 において、ショップサーバ 2 3 - 1 の閲覧プログラム 1 2 3 は、通信ネットワーク 4 を介して、電話機一体型端末機 5 0 1 に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップ S 2 1 0 4 において、電話機一体型端末機 5 0 1 の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部 6 0 6 に表示させ、使用者に閲覧させる。また、電話機一体型端末機 5 0 1 のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部 6 0 7 に再生させて、使

用者に試聴させたり、または、キーワードにより所望のコンテンツをショップサーバ23-1の閲覧プログラム123に検索させ、その結果を表示部606に表示させる。

【0156】

ステップS2402およびステップS2104の処理は、電話機一体型端末機501の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【0157】

ステップS2105において、電話機一体型端末機501のブラウザプログラムは、通信ネットワーク4を介して、購入依頼をショップサーバ23-1に送信する。ステップS2403において、ショップサーバ23-1の閲覧プログラム123は、電話機一体型端末機501から送信された購入依頼を受信する。

【0158】

ステップS2404において、ショップサーバ23-1のコンテンツ情報送信プログラム122は、ステップS2403の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ22-1のURL、およびコンテンツを特定するためのコンテンツIDなどを含む、コンテンツ情報を、通信ネットワーク4を介して、電話機一体型端末機501に送信する。ステップS2106において、電話機一体型端末機501のコンテンツ情報受信プログラム727は、ショップサーバ23-1が送信した、コンテンツ情報を受信する。

【0159】

ステップS2405において、ショップサーバ23-1の鍵情報送信プログラム121は、ステップS2403の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ21-1のURLなどの、鍵情報を通信ネットワーク4を介して、電話機一体型端末機501に送信する。ステップS2107において、電話機一体型端末機501の鍵情報受信プログラム726は、ショップサーバ23-1が送信した、鍵情報を受信する。

【0160】

ステップS2108において、電話機一体型端末機501のIP通信プログラ



ム 7 0 1 は、予め記録している代理サーバ 5 0 3 の URL を基に、代理サーバ 5 0 3 と IP 通信を確立する。ステップ S 2 5 0 1 において、代理サーバ 5 0 3 の IP 通信プログラム 7 5 1 は、電話機一体型端末機 5 0 1 と IP 通信を確立する。

#### 【 0 1 6 1 】

ステップ S 2 1 0 9 において、電話機一体型端末機 5 0 1 のライセンス管理プログラム 7 1 1 のサーバ認証プログラム 7 2 2 は、代理サーバ 5 0 3 を認証する。ステップ S 2 5 0 2 において、代理サーバ 5 0 3 のライセンス管理プログラム 7 6 1 の PD 認証プログラム 7 8 2 は、電話機一体型端末機 5 0 1 を認証する。

#### 【 0 1 6 2 】

ステップ S 2 1 0 9 およびステップ S 2 5 0 2 における電話機一体型端末機 5 0 1 と代理サーバ 5 0 3 との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップ S 1 1 2 およびステップ S 6 0 2 における鍵サーバ 2 1 - 1 とパーソナルコンピュータ 1 との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機 5 0 1 および代理サーバ 5 0 3 は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

#### 【 0 1 6 3 】

ステップ S 2 1 0 9 およびステップ S 2 5 0 2 における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機 5 0 1 がコンテンツをダウンロードする処理は、コンテンツをダウンロードしないで、終了する。

#### 【 0 1 6 4 】

ステップ S 2 1 1 0 において、電話機一体型端末機 5 0 1 のコンテンツ管理プログラム 7 2 5 は、コンテンツ ID を代理サーバ 5 0 3 に送信する。ステップ S 2 5 0 3 において、代理サーバ 5 0 3 は、電話機一体型端末機 5 0 1 が送信したコンテンツ ID を受信する。ステップ S 2 1 1 1 において、電話機一体型端末機 5 0 1 の鍵管理プログラム 7 2 4 は、ステップ S 2 1 0 7 の処理で受信した鍵情報を代理サーバ 5 0 3 に送信する。ステップ S 2 5 0 4 において、代理サーバ 5

03は、電話機一体型端末機501が送信した、鍵情報を受信する。

【0165】

ステップS2505において、代理サーバ503のシステム識別プログラム773は、ステップS2503の処理で受信したコンテンツIDを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ5-1であることを識別する。

【0166】

なお、ステップS2110において、電話機一体型端末機501は、コンテンツIDと共にコンテンツサーバ22-1のURLを送信して、ステップS2503において、代理サーバ503は、コンテンツIDと共にコンテンツサーバ22-1のURLを受信するようにしてもよい。

【0167】

ステップS2506において、代理サーバ503のIP通信プログラム751は、ステップS2505の処理の識別の結果を基に、コンテンツサーバ22-1とIP通信を確立する。ステップS2601において、コンテンツサーバ22-1のIP通信プログラム193は、代理サーバ503とIP通信を確立する。

【0168】

ステップS2507において、代理サーバ503のコンテンツ管理プログラム772は、ステップS2503の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-1に送信する。ステップS2602において、コンテンツサーバ22-1は、代理サーバ503が送信したコンテンツIDを受信する。ステップS2603において、コンテンツサーバ22-1のコンテンツ配信プログラム192は、ステップS2602で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム191から読み出して、通信ネットワーク4を介して、代理サーバ503に配信する。

【0169】

ステップS2508において、代理サーバ503のコンテンツ管理プログラム772の受信プログラム785は、コンテンツサーバ22-1が送信したコンテ

ンツを受信する。

【0170】

ステップS2509において、代理サーバ503のIP通信プログラム751は、ステップS2505の処理の識別の結果を基に、鍵サーバ21-1とIP通信を確立する。ステップS2701において、鍵サーバ21-1のIP通信プログラム155は、代理サーバ503とIP通信を確立する。

【0171】

ステップS2510において、代理サーバ503のライセンス管理プログラム761のサーバ認証プログラム781は、鍵サーバ21-1を認証する。ステップS2702において、鍵サーバ21-1の認証プログラム151は、代理サーバ503を認証する。

【0172】

例えば、鍵サーバ21-1には、マスター鍵KMSSが予め記憶されており、代理サーバ503には、個別鍵KPCCと代理サーバ503のIDが予め記憶されている。代理サーバ503には、更に、マスター鍵KMCCが予め記憶されており、鍵サーバ21-1にも鍵サーバ21-1のIDと個別鍵KPSSが記憶されている。

【0173】

鍵サーバ21-1は、代理サーバ503から、代理サーバ503のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSSにハッシュ関数を適用して、代理サーバ503の個別鍵KPCCと同一の鍵を生成する。

【0174】

代理サーバ503は、鍵サーバ21-1から、鍵サーバ21-1のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMCCにハッシュ関数を適用して、鍵サーバ21-1の個別鍵KPSSと同一の鍵を生成する。このようにすることで、代理サーバ503と鍵サーバ21-1の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【0175】

ステップS2510またはステップS2702における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

## 【0176】

ステップS2511において、代理サーバ503の鍵管理プログラム771は、ステップS2503の処理で取得したコンテンツIDを鍵サーバ21-1に送信する。ステップS2703において、鍵サーバ21-1は、代理サーバ503が送信したコンテンツIDを受信する。ステップS2704において、鍵サーバ21-1の鍵配信プログラム152は、鍵保存プログラム153がコンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（鍵サーバ21-1と代理サーバ503とで共有する一時鍵で暗号化されている）を代理サーバ503に送信する。ステップS2512において、代理サーバ503の鍵管理プログラム771の鍵受信プログラム783は、鍵サーバ21-1が送信したコンテンツ鍵を受信する。

## 【0177】

ステップS2513において、代理サーバ503の鍵管理プログラム771の鍵配信プログラム784は、ステップS2512の処理で受信したコンテンツ鍵を、鍵サーバ21-1と代理サーバ503とで共有する一時鍵で復号し、電話機一体型端末機501と代理サーバ503で共有する一時鍵で暗号化して、通信ネットワーク4を介して、暗号化されているコンテンツ鍵を電話機一体型端末機501に送信する。ステップS2112において、電話機一体型端末機501の鍵管理プログラム724の受信プログラム731は、代理サーバ503が送信したコンテンツ鍵を受信する。鍵管理プログラム724は、コンテンツ鍵を電話機一体型端末機501と代理サーバ503で共有する一時鍵で復号して、ポータブルメディア3-1の鍵管理プログラム102に供給し、鍵管理プログラム102に、コンテンツ鍵を記憶させる。

## 【0178】

ステップS2514において、代理サーバ503のコンテンツ管理プログラム772のコンテンツ配信プログラム786は、通信ネットワーク4を介して、暗号化されているコンテンツを電話機一体型端末機501に送信する。ステップS2113において、電話機一体型端末機501のコンテンツ管理プログラム725の受信プログラム732は、代理サーバ503が送信したコンテンツを受信す

る。

【0179】

ステップS2114において、電話機一体型端末機501のPHS/IMT通信プログラム703は、公衆回線網31との接続を切断する。ステップS2202において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を切断する。

【0180】

ステップS2115において、電話機一体型端末機501のフォーマット管理プログラム713は、ステップS2113の処理で受信したコンテンツのフォーマットを変換する。コンテンツ管理プログラム725は、フォーマットを変換したコンテンツを、インターフェース609を介して、ポータブルメディア3-1に供給して、コンテンツ管理プログラム103に、コンテンツを記憶させ、処理は終了する。

【0181】

次に、電話機一体型端末機501がサーバ5-2からコンテンツをダウンロードする処理を図13および図14のフローチャートを参照して説明する。ステップS3101乃至ステップS3504の処理は、サーバ5-2、並びにIP通信プログラム701、ISP接続プログラム702、PHS/IMT通信プログラム703、およびダウンロードプログラム712により実行され、それぞれ、ステップS2101乃至ステップS2504の処理と同様なので、その説明は省略する。

【0182】

ステップS3505において、代理サーバ503のシステム識別プログラム773は、ステップS3503の処理で受信したコンテンツIDを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ5-2であることを識別する。

【0183】

ステップS3506において、代理サーバ503のIP通信プログラム751は、ステップS3505の識別の処理の結果を基に、鍵サーバ21-2とIP通

信を確立する。ステップS3701において、鍵サーバ21-2は、代理サーバ503とIP通信を確立する。

【0184】

ステップS3507において、代理サーバ503のサーバ認証プログラム781は、鍵サーバ21-2を認証する。ステップS3702において、鍵サーバ21-2は、代理サーバ503を認証する。

【0185】

ステップS3507およびステップS3702の処理は、ステップS2510およびステップS2702の処理と同様の処理である。

【0186】

ステップS3507またはステップS3702における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【0187】

ステップS3508において、代理サーバ503の鍵管理プログラム771は、ステップS3503の処理で取得したコンテンツIDを鍵サーバ21-2に送信する。ステップS3703において、鍵サーバ21-2は、代理サーバ503が送信したコンテンツIDを受信する。ステップS3704において、鍵サーバ21-2は、コンテンツIDと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク4を介して、そのコンテンツ鍵（鍵サーバ21-2と代理サーバ503とで共有する一時鍵で暗号化されている）を代理サーバ503に送信する。ステップS3509において、代理サーバ503の鍵管理プログラム771の鍵受信プログラム783は、鍵サーバ21-2が送信したコンテンツ鍵を受信する。

【0188】

ステップS3510において、代理サーバ503のIP通信プログラム751は、ステップS3505の識別の処理の結果を基に、コンテンツサーバ22-2とIP通信を確立する。ステップS3601において、コンテンツサーバ22-2は、代理サーバ503とIP通信を確立する。

【0189】

ステップS3511において、代理サーバ503のコンテンツ管理プログラム772は、ステップS3503の処理で取得したコンテンツIDを、通信ネットワーク4を介して、コンテンツサーバ22-2に送信する。ステップS3602において、コンテンツサーバ22-2は、代理サーバ503が送信したコンテンツIDを受信する。ステップS3603において、コンテンツサーバ22-2は、ステップS3602で受信したコンテンツIDに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク4を介して、代理サーバ503に配信する。

## 【0190】

ステップS3512において、代理サーバ503のコンテンツ管理プログラム772の受信プログラム785は、コンテンツサーバ22-2が送信したコンテンツを受信する。

## 【0191】

ステップS3512乃至ステップS3115の処理は、ステップS2513乃至ステップS2115の処理と同様なので、その説明は省略する。

## 【0192】

以上のように、電話機一体型端末機501は、代理サーバ503を介することにより、サーバ5-1からコンテンツおよびコンテンツ鍵をダウンロードするときも、サーバ5-2からコンテンツおよびコンテンツ鍵をダウンロードするときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を受信してから、コンテンツを受信する）で、コンテンツおよびコンテンツ鍵を受信することができる。

## 【0193】

また、図11乃至図14のフローチャートを参照して説明した手順は、後述する代理サーバ503がコンテンツの符号化方式および暗号化方式を変換する処理（図16および図17のフローチャートを参照して説明する）に比較して、電話機一体型端末機501が公衆回線網31に接続している時間を短くすることができる。

## 【0194】

次に、図15を参照して、本願のデジタルデータ伝送システムの他の機能の構成について説明する。図10で説明した構成の場合と同一の部分には、図10の場合と同一の番号を付してあり、その説明は省略する。

## 【0195】

図15に示す電話機一体型端末機501は、フォーマット管理プログラム713を有しない。

## 【0196】

図15に示す代理サーバ503のサーバ用LCM514は、ライセンス管理プログラム761およびシーケンス管理プログラム762に加えて、フォーマット管理プログラム801を含む。

## 【0197】

フォーマット管理プログラム801は、コンテンツサーバ22-1または22-2からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム801は、システム識別プログラム811およびフォーマット変換プログラム812から構成されている。

## 【0198】

システム識別プログラム811は、コンテンツのダウンロード先が、サーバ5-1であるか、サーバ5-2であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム812は、コンテンツの符号化方式および暗号化方式を変換する。

## 【0199】

次に、図15にその構成を示す電話機一体型端末機501および代理サーバ503がサーバ5-2からコンテンツをダウンロードする処理を図16および図17のフローチャートを参照して説明する。

## 【0200】

ステップS4101乃至ステップS4512の処理は、それぞれ、ステップS3101乃至ステップS3512の処理と同様なので、その説明は省略する。

## 【0201】

ステップS4512において、代理サーバ503のフォーマット管理プログラ



ム801は、ステップS4512の処理で受信したコンテンツのフォーマットを変換する。

#### 【0202】

ステップS4514において、代理サーバ503の鍵管理プログラム771の鍵配信プログラム784は、ステップS4509の処理で受信したコンテンツ鍵を、鍵サーバ21-2と代理サーバ503とで共有する一時鍵で復号し、電話機一体型端末機501と代理サーバ503で共有する一時鍵で暗号化して、通信ネットワーク4を介して、暗号化されているコンテンツ鍵を電話機一体型端末機501に送信する。ステップS4112において、電話機一体型端末機501の鍵管理プログラム724の受信プログラム731は、代理サーバ503が送信したコンテンツ鍵を受信する。鍵管理プログラム724は、コンテンツ鍵を電話機一体型端末機501と代理サーバ503で共有する一時鍵で復号して、ポータブルメディア3-1の鍵管理プログラム102に供給し、鍵管理プログラム102に、コンテンツ鍵を記憶させる。

#### 【0203】

ステップS4515において、代理サーバ503のコンテンツ管理プログラム772のコンテンツ配信プログラム786は、通信ネットワーク4を介して、暗号化されているコンテンツを電話機一体型端末機501に送信する。ステップS4113において、電話機一体型端末機501のコンテンツ管理プログラム725の受信プログラム732は、代理サーバ503が送信したコンテンツを受信する。コンテンツ管理プログラム725は、受信したコンテンツ（フォーマットが変換されている）を、インターフェース609を介して、ポータブルメディア3-1に供給して、コンテンツ管理プログラム103に、コンテンツを記憶させる。

#### 【0204】

ステップS4114において、電話機一体型端末機501のPHS/IMT通信プログラム703は、公衆回線網31との接続を切断する。ステップS4202において、公衆回線網31の図示せぬ地上局などは、電話機一体型端末機501と接続を切断して、処理は終了する。

## 【 0 2 0 5 】

なお、サーバ 5 - 1 からコンテンツおよびコンテンツ鍵を受信する処理は、代理サーバ 5 0 3 がサーバ 5 - 1 よりコンテンツを受信した後、サーバ 5 - 1 よりコンテンツ鍵を受信する手順となり、同様に行われる。

## 【 0 2 0 6 】

このように、代理サーバ 5 0 3 は、サーバ 5 - 1 または 5 - 2 から受信したコンテンツの符号化方式および暗号化方式を変換して、電話機一体型端末機 5 0 1 に供給することもできる。この場合、電話機一体型端末機 5 0 1 は、コンテンツの符号化方式および暗号化方式を変換するプログラムが不要となる。従って、電話機一体型端末機 5 0 1 は、図 1 0 に示す場合に比較して、より少ない演算能力または記憶容量でも、迅速にコンテンツを受信する処理を実行することができる。

## 【 0 2 0 7 】

また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画像のデータ、テキストのデータ、またはプログラムなどでもよい。

## 【 0 2 0 8 】

なお、電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 が、コンテンツをダウンロードすると説明したが、電話機一体型端末機 5 0 1 またはパーソナルコンピュータ 5 0 2 に限らず、携帯電話機、PDA (Personal Digital Assistant)、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

## 【 0 2 0 9 】

また、電話機一体型端末機 5 0 1 は、PHS または IMT により通信すると説明したが、PHS または IMT に限らず、W-CDMA (Code Division Multiple Access)、衛星通信、衛星放送、PSTN (Public Switched telephone network)、xDSL (x Digital Subscriber Line)、ISDN (Integrated Services Digital Network)、またはプライベートネットワークなどで通信するようにしてもよい。

## 【 0 2 1 0 】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

## 【 0 2 1 1 】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図 8 または図 9 に示すように、磁気ディスク 6 4 1 若しくは磁気ディスク 6 8 1 (いずれもフロッピーディスクを含む)、光ディスク 6 4 2 若しくは光ディスク 6 8 2 (いずれも、CD-ROM (Compact Disc-Read Only Memory)、DVD (Digital Versatile Disc)を含む)、光磁気ディスク 6 4 3 若しくは光磁気ディスク 6 8 3 (いずれもMD (Mini-Disc)を含む)、若しくは半導体メモリ 6 4 4 若しくは半導体メモリ 6 8 4 などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM 6 0 2 若しくはROM 6 5 2 や、HDD 6 6 1 などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部 6 0 8 または通信部 6 6 3 を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

## 【 0 2 1 2 】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

## 【 0 2 1 3 】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

## 【 0 2 1 4 】

## 【発明の効果】

請求項 1 に記載の情報提供装置、請求項 3 に記載の情報提供方法、および請求項 4 に記載のプログラム格納媒体によれば、第 1 の情報処理装置が認証され、第 2 の情報処理装置または第 3 の情報処理装置が認証され、第 1 の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第 2 の情報処理装置を特定するデータまたは第 3 の情報処理装置を特定するデータの受信が制御され、第 2 の情報処理装置を特定するデータを受信した場合、第 2 の情報処理装置に対応した手順で、第 2 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 2 の情報処理装置からコンテンツおよび鍵を受信し、第 3 の情報処理装置を特定するデータを受信した場合、第 3 の情報処理装置に対応した手順で、第 3 の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第 3 の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第 1 の情報処理装置へのコンテンツおよび鍵の送信が制御されるようにしたので、第 1 の情報処理装置の処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

## 【0 2 1 5】

請求項 5 に記載の情報処理装置、請求項 6 に記載の情報処理方法、および請求項 7 に記載のプログラム格納媒体によれば、第 1 の情報提供装置が認証され、第 1 の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第 2 の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第 3 の情報提供装置を特定するデータのいずれかの送信が制御され、第 2 の情報提供装置または第 3 の情報提供装置から第 1 の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御されるようにしたので、処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

## 【図面の簡単な説明】

## 【図 1】

従来のデジタルデータ伝送システムの構成を示す図である。

## 【図 2】

従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図3】

パーソナルコンピュータ1がサーバ5-1からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図4】

パーソナルコンピュータ1がサーバ5-1からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図5】

パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図6】

パーソナルコンピュータ1がサーバ5-2からコンテンツをダウンロードして、ポータブルデバイス2にチェックアウトする従来の処理を説明するフローチャートである。

【図7】

本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図8】

電話機一体型端末機501の構成を説明する図である。

【図9】

代理サーバ503の構成を説明する図である。

【図10】

本願のデジタルデータ伝送システムの機能の構成を説明する図である。

【図11】

電話機一体型端末機501がサーバ5-1からコンテンツをダウンロードする処理を説明するフローチャートである。

【図12】

電話機一体型端末機 501 がサーバ 5-1 からコンテンツをダウンロードする処理を説明するフローチャートである。

【図 13】

電話機一体型端末機 501 がサーバ 5-2 からコンテンツをダウンロードする処理を説明するフローチャートである。

【図 14】

電話機一体型端末機 501 がサーバ 5-2 からコンテンツをダウンロードする処理を説明するフローチャートである。

【図 15】

本願のデジタルデータ伝送システムの他の機能の構成を説明する図である。

【図 16】

電話機一体型端末機 501 がサーバ 5-2 からコンテンツをダウンロードする処理を説明するフローチャートである。

【図 17】

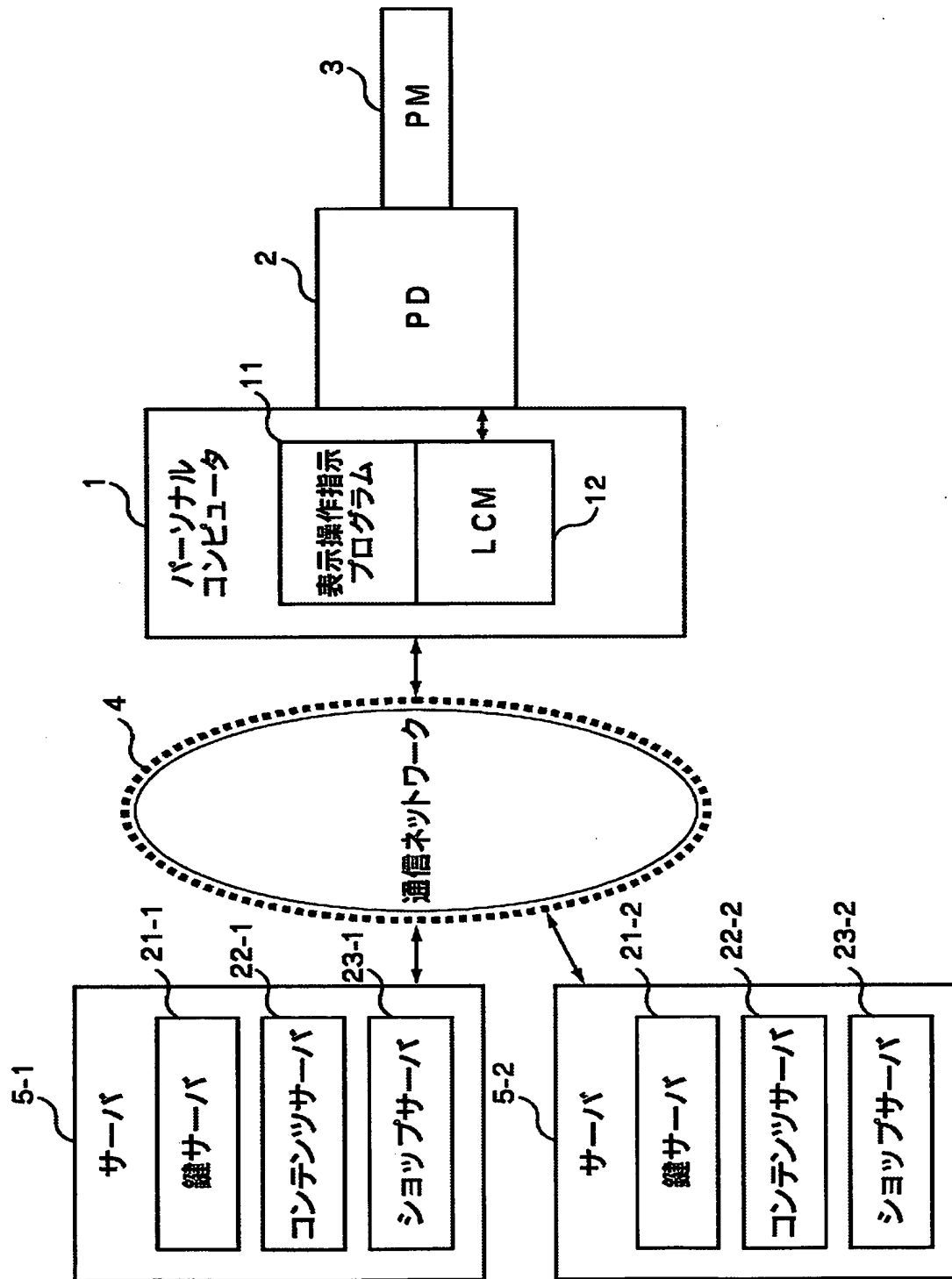
電話機一体型端末機 501 がサーバ 5-2 からコンテンツをダウンロードする処理を説明するフローチャートである。

【符号の説明】

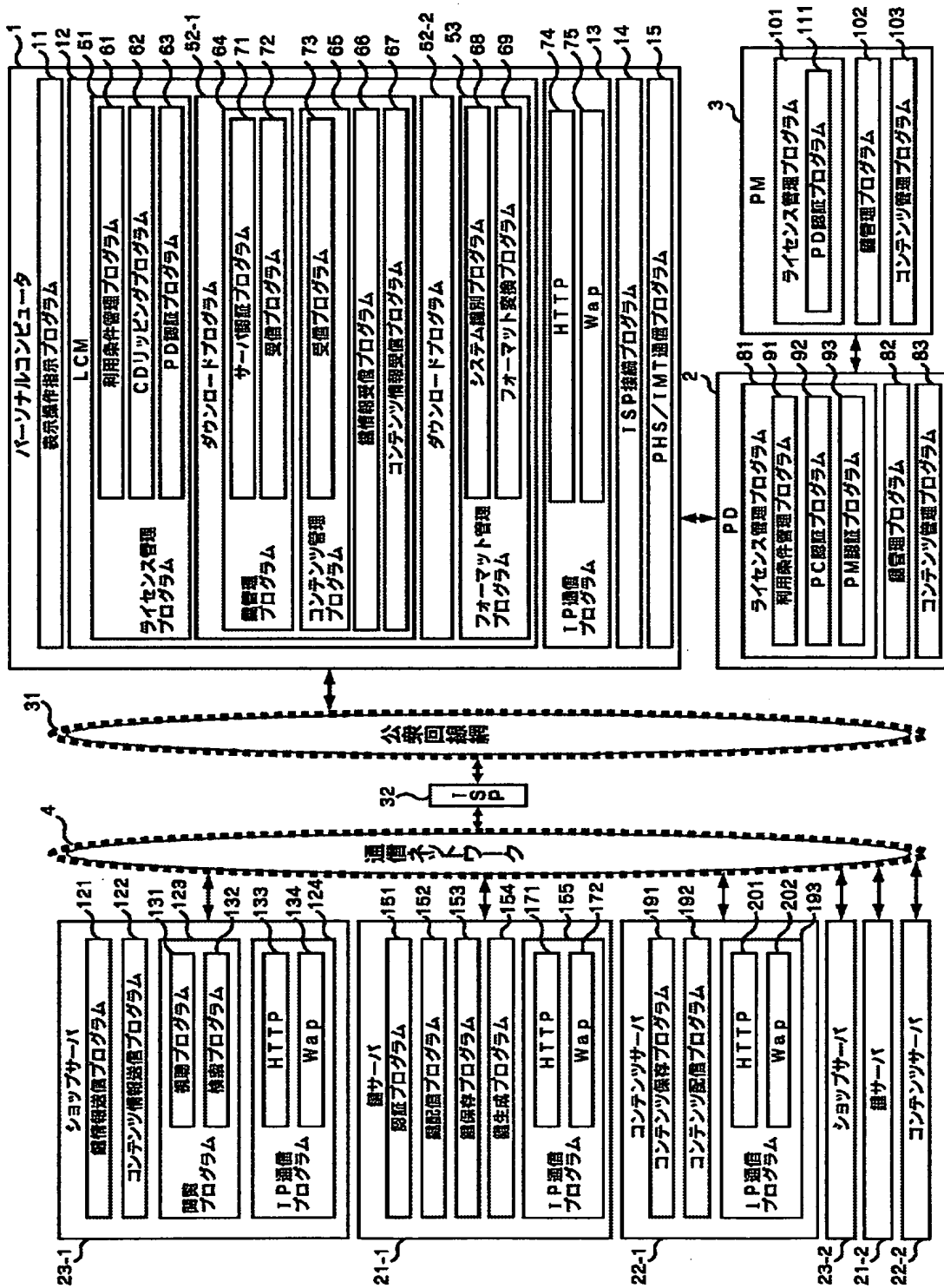
501 電話機一体型端末機, 503 代理サーバ, 511 表示操作指示プログラム, 512 クライアント用 LCM, 514 サーバ用 LCM, 601 CPU, 602 ROM, 603 RAM, 608 通信部, 641 磁気ディスク, 642 光ディスク, 643 光磁気ディスク, 644 半導体メモリ, 651 CPU, 652 ROM, 653 RAM, 663 通信部, 681 磁気ディスク, 682 光ディスク, 683 光磁気ディスク, 684 半導体メモリ

【書類名】図面

【図 1】



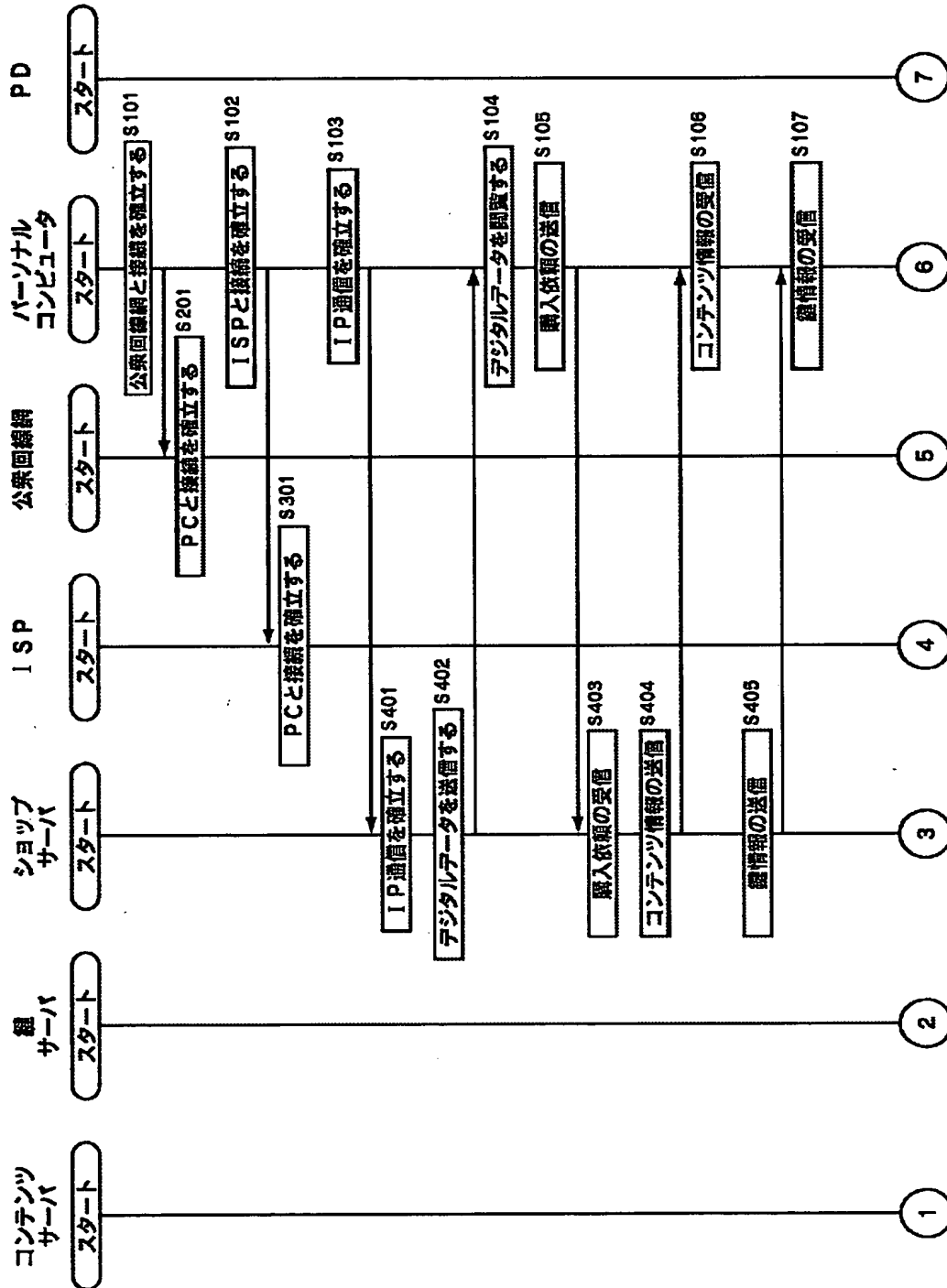
【図 2】



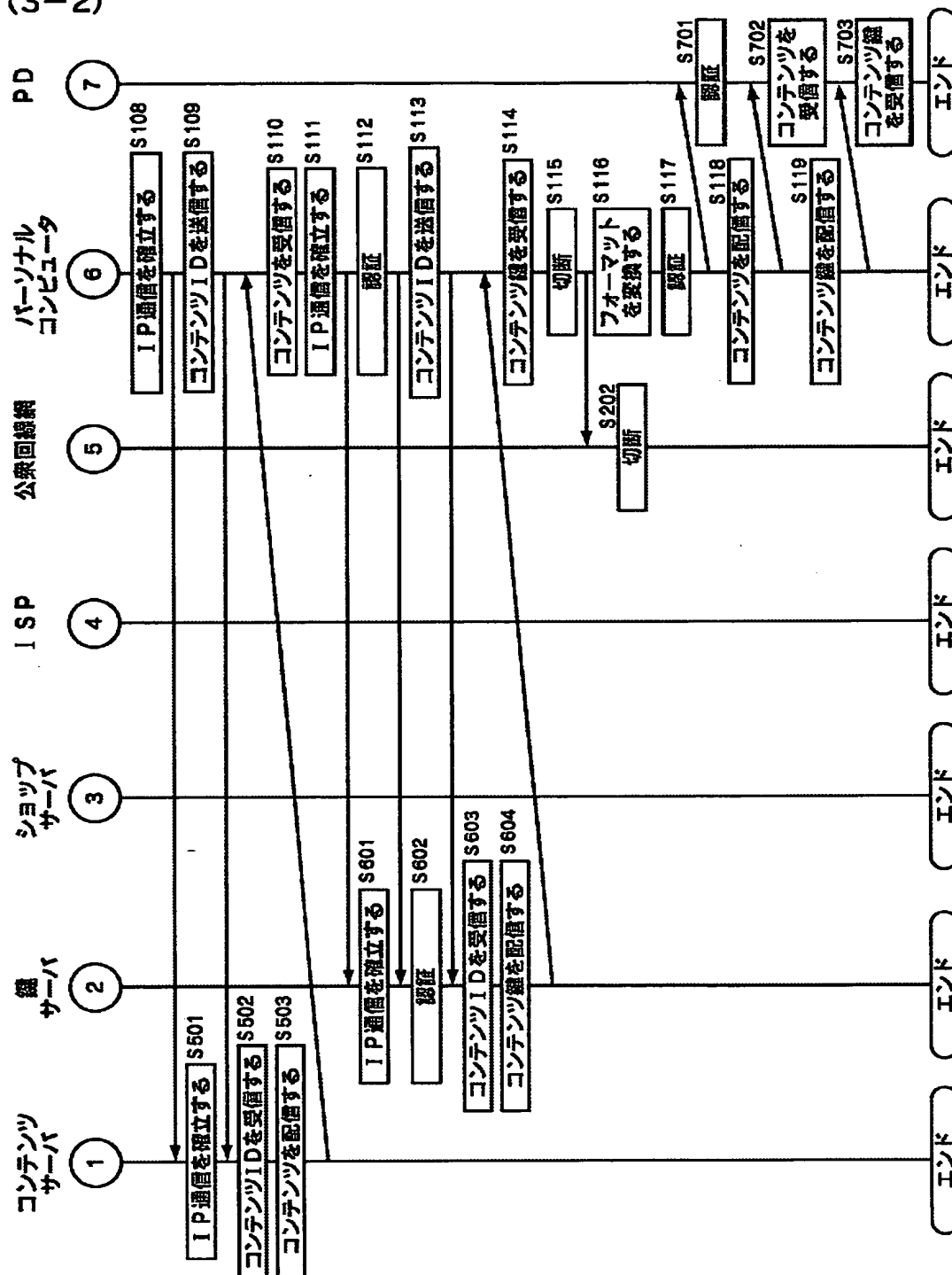


【図 3】

(3-1)

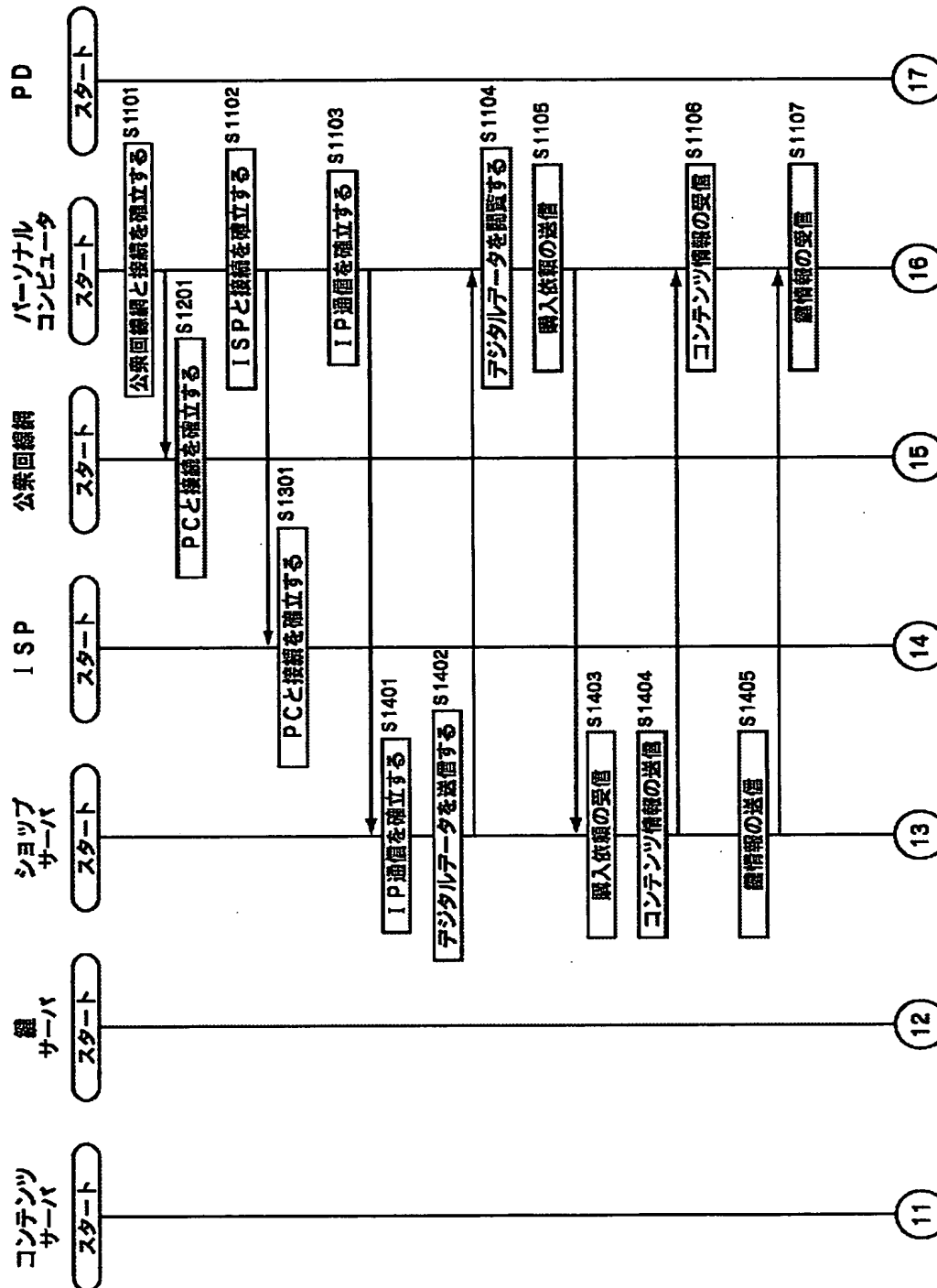


(3-2)



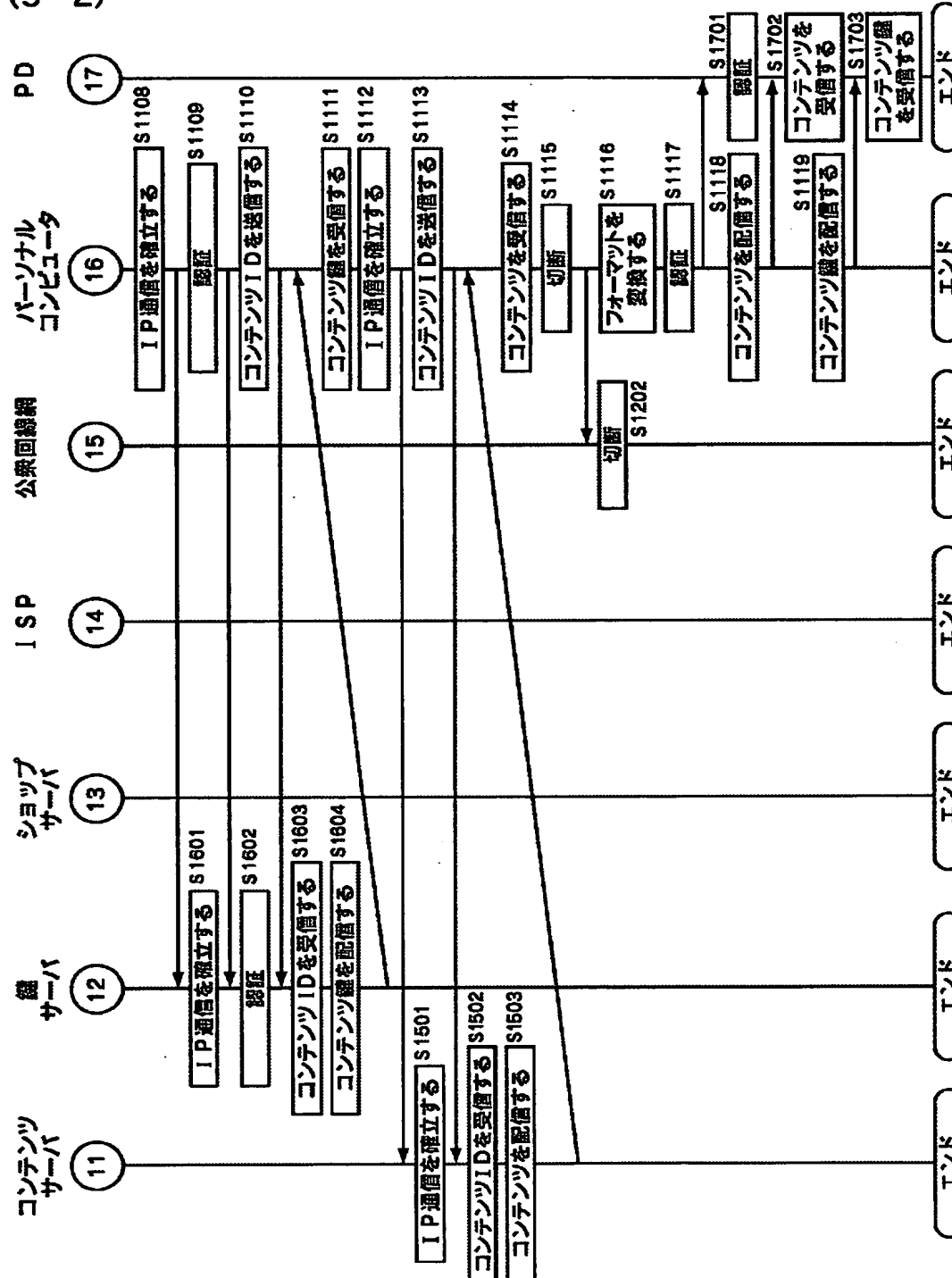
【図 5】

(5-1)

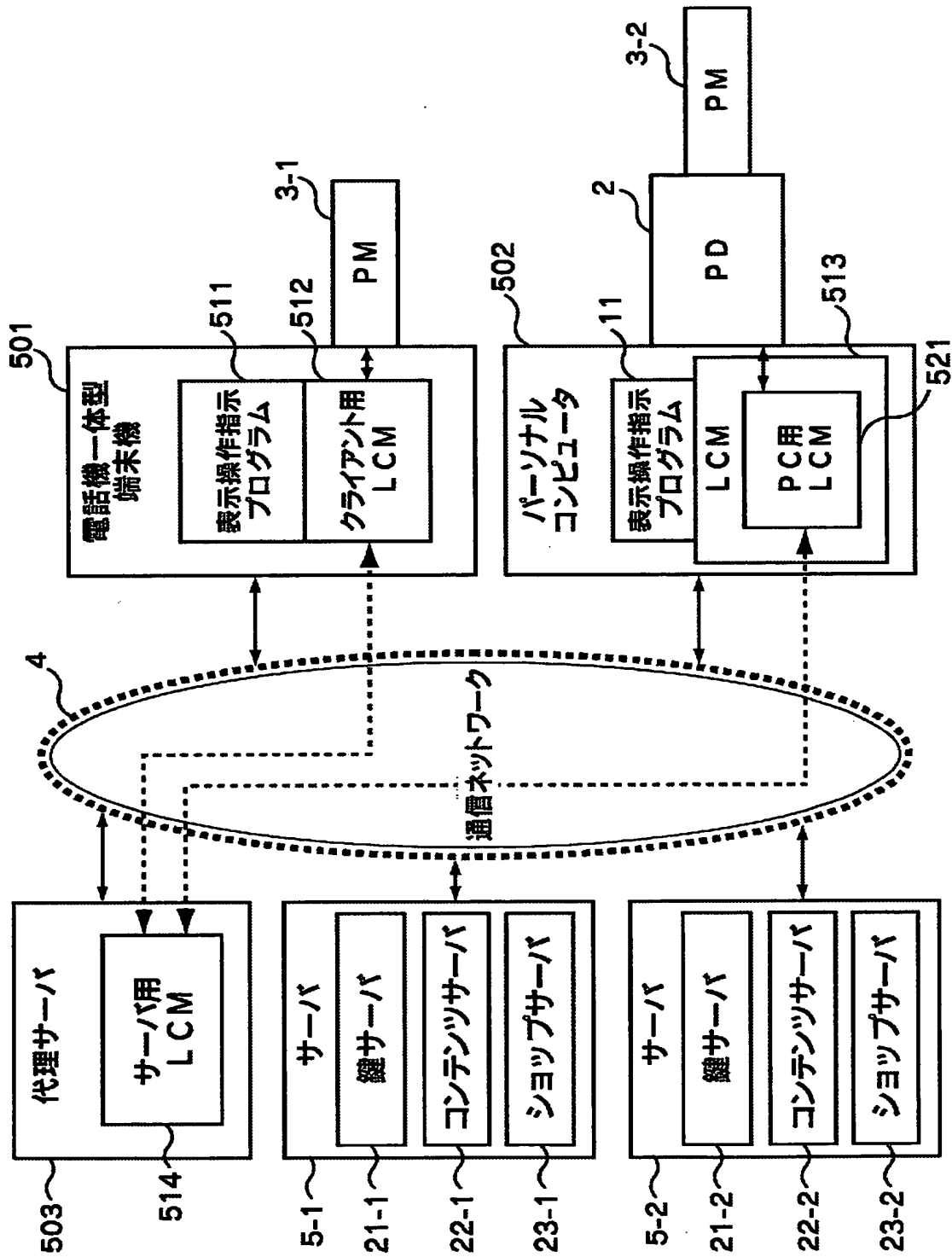


【図 6】

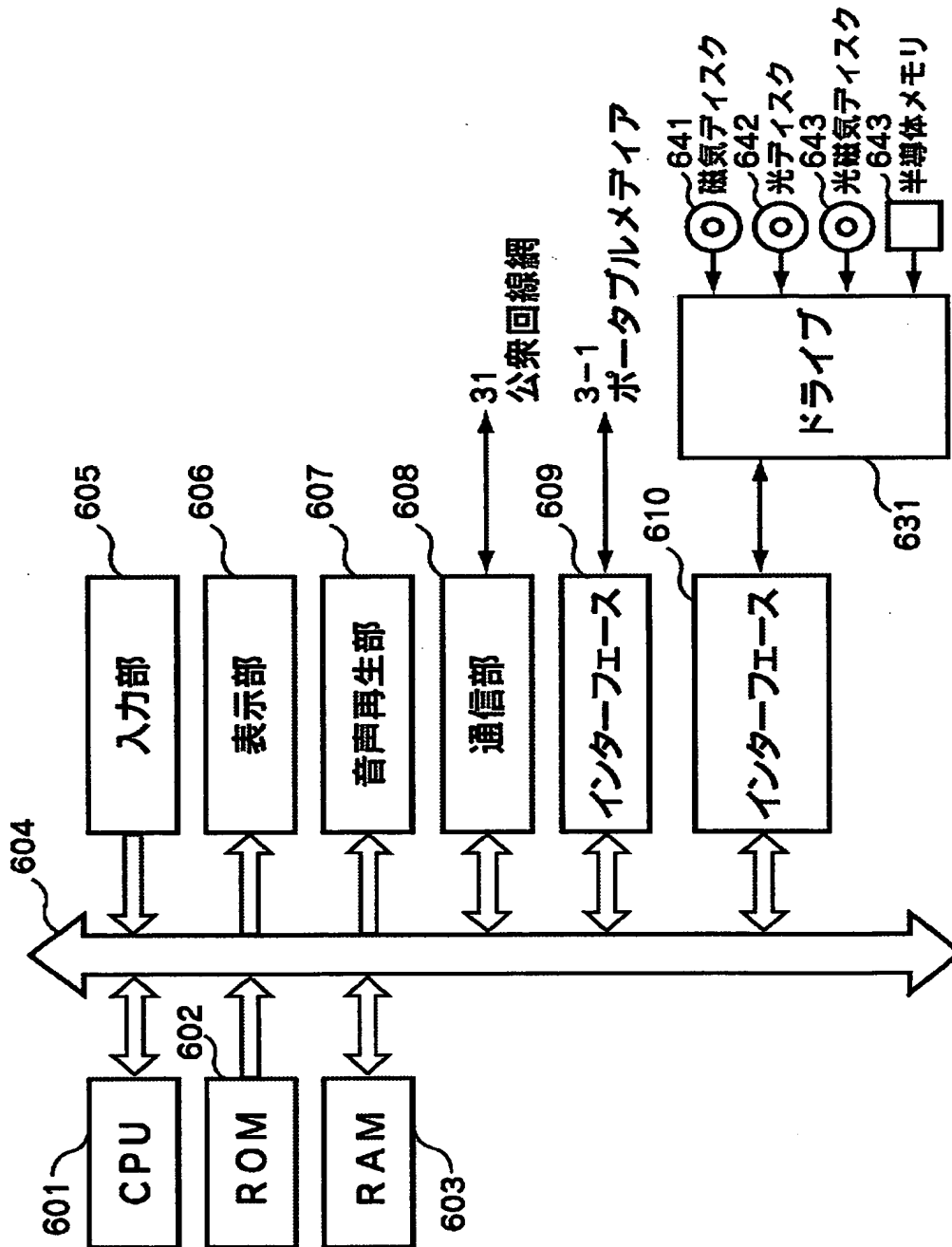
(5-2)



【図7】

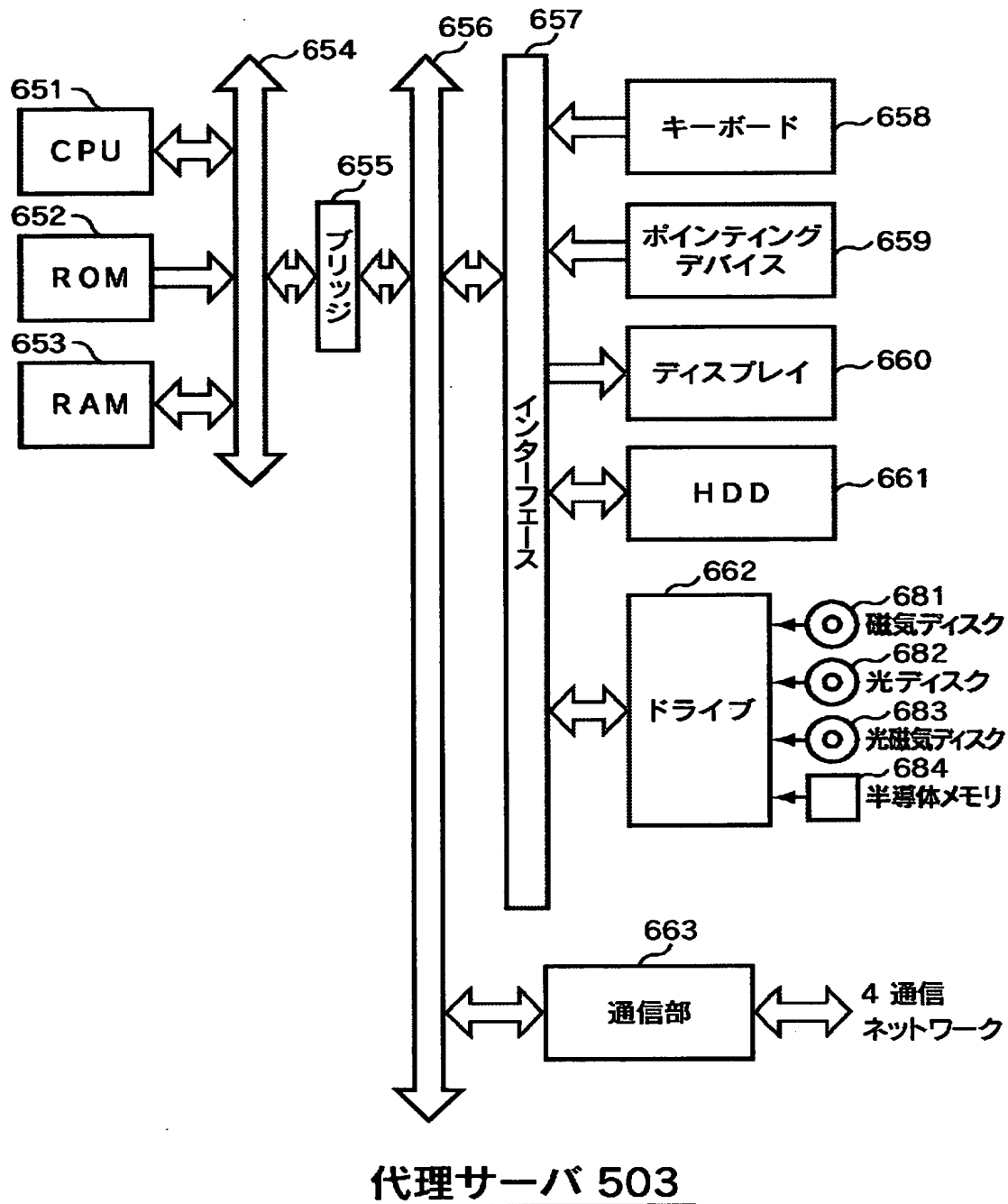


【図 8】

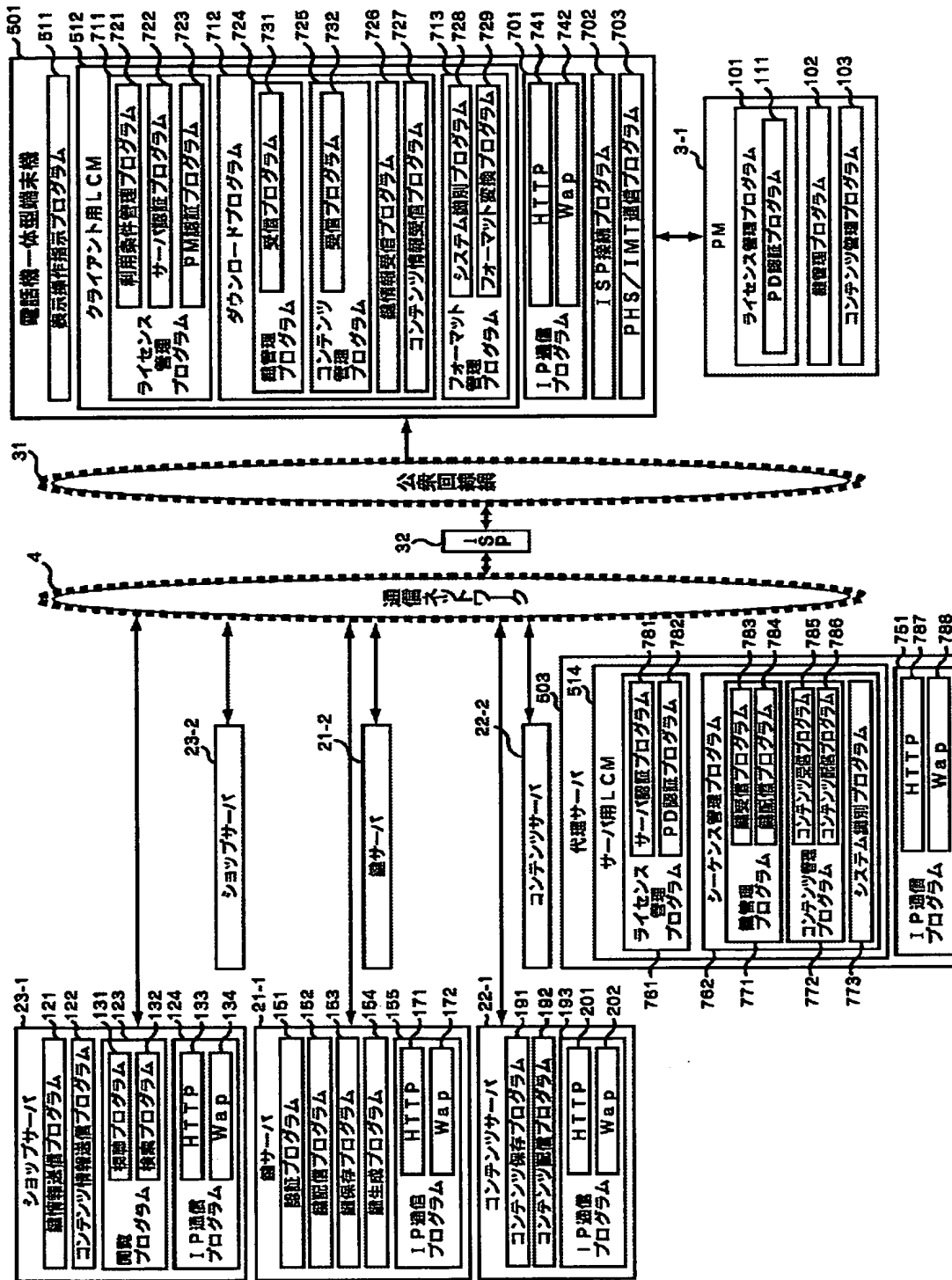


電話機一体型端末機 501

【図 9】



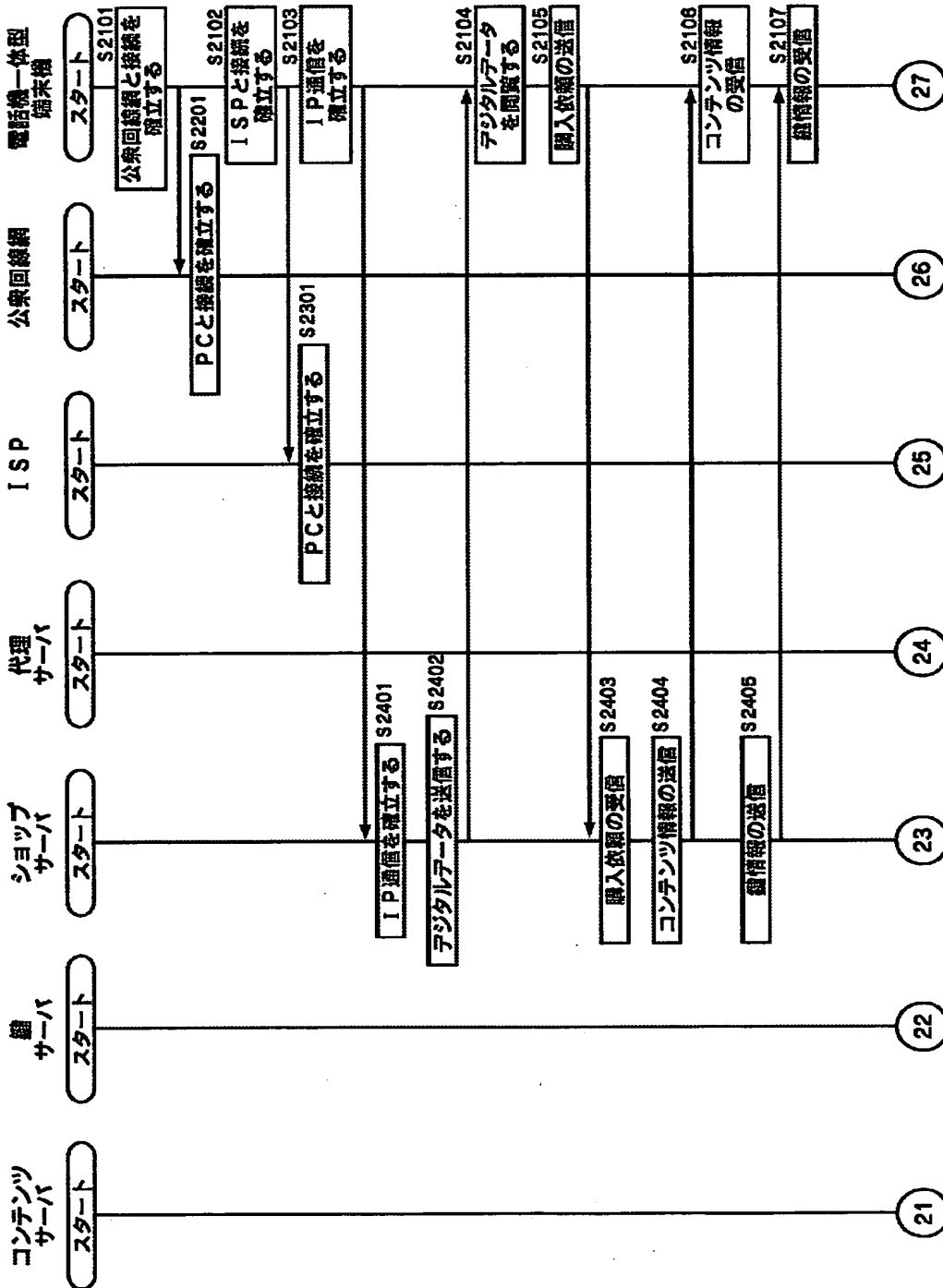
【図 10】





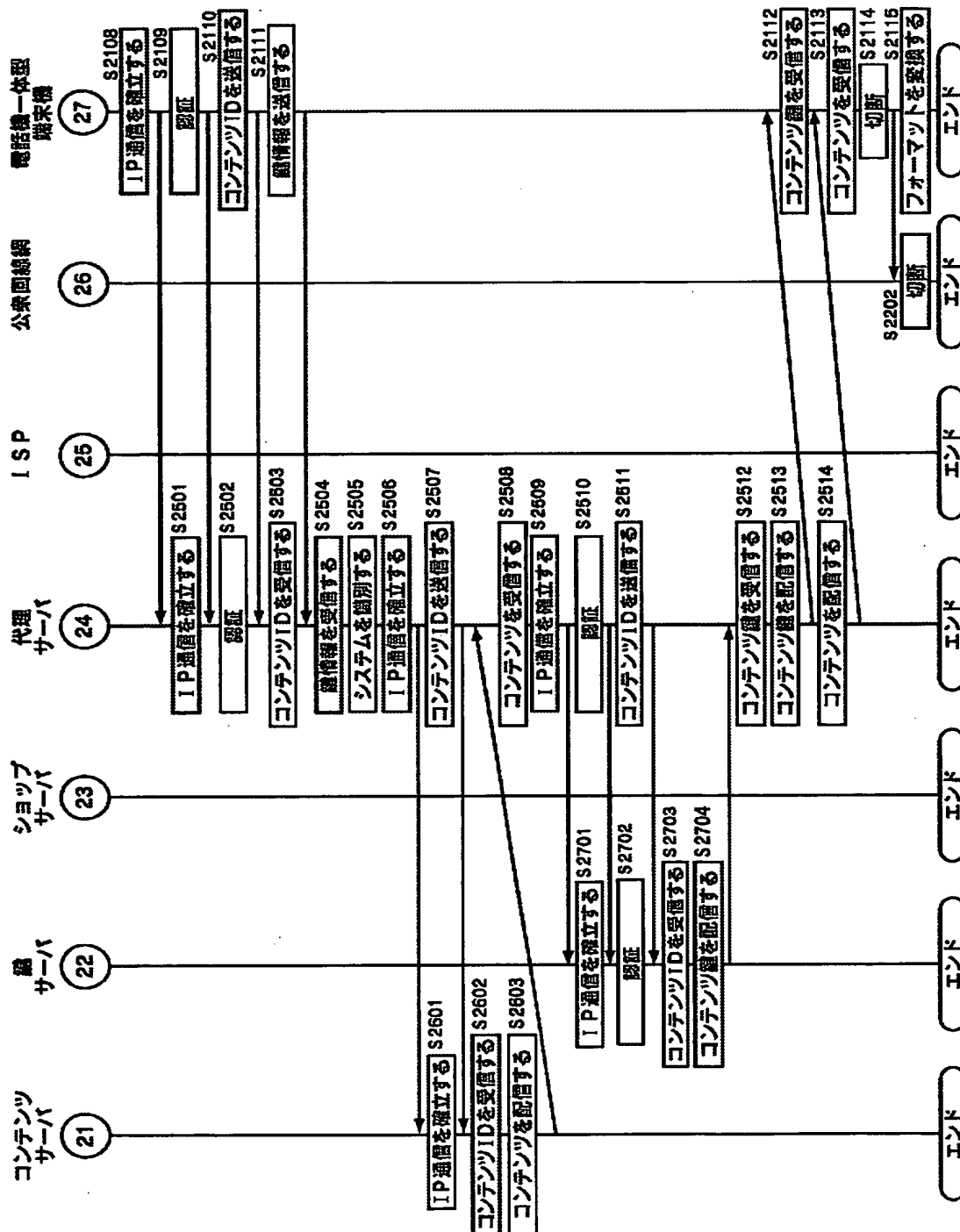
【図 11】

(11-1)



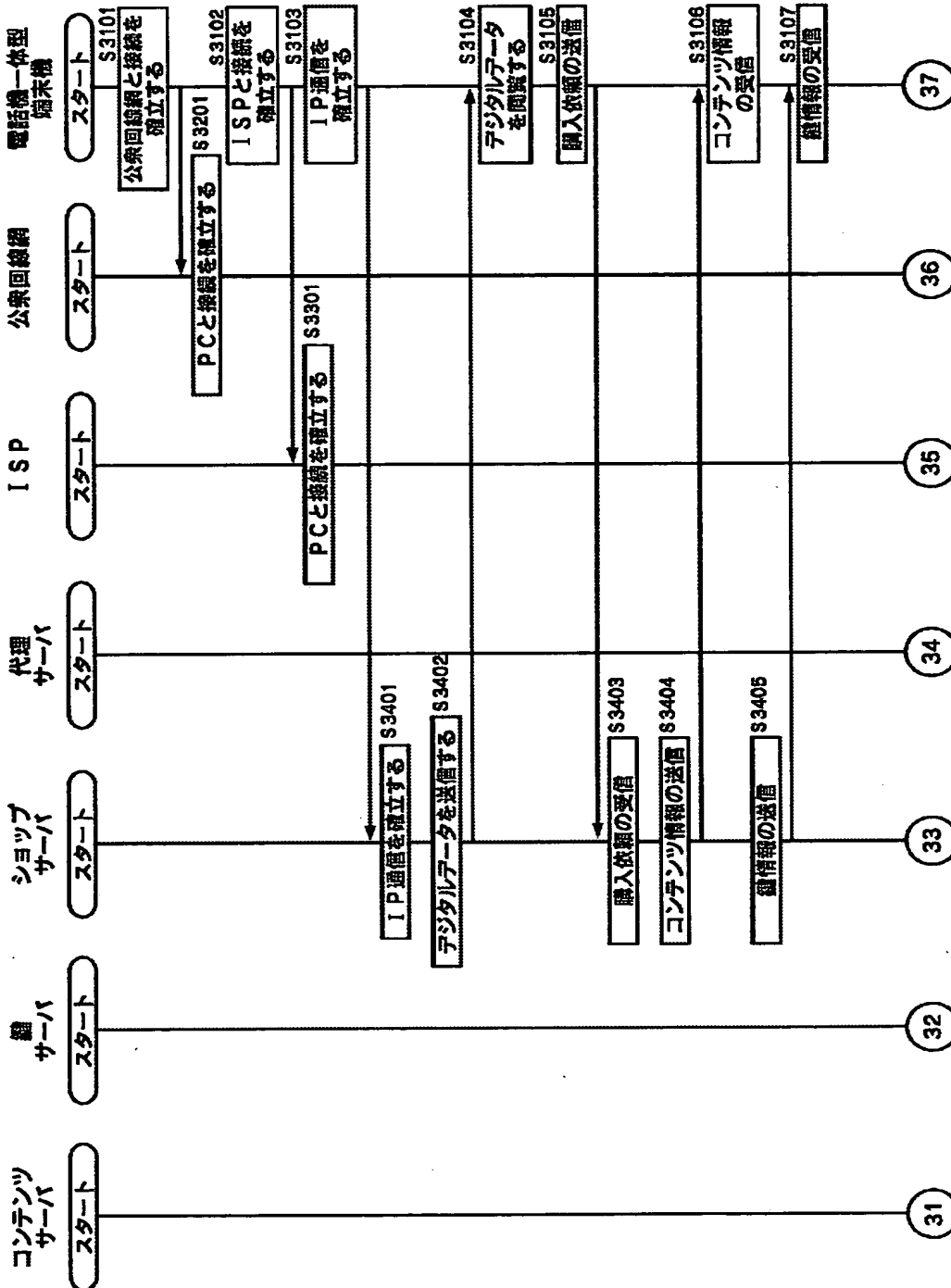
【圖 12】

(11-2)



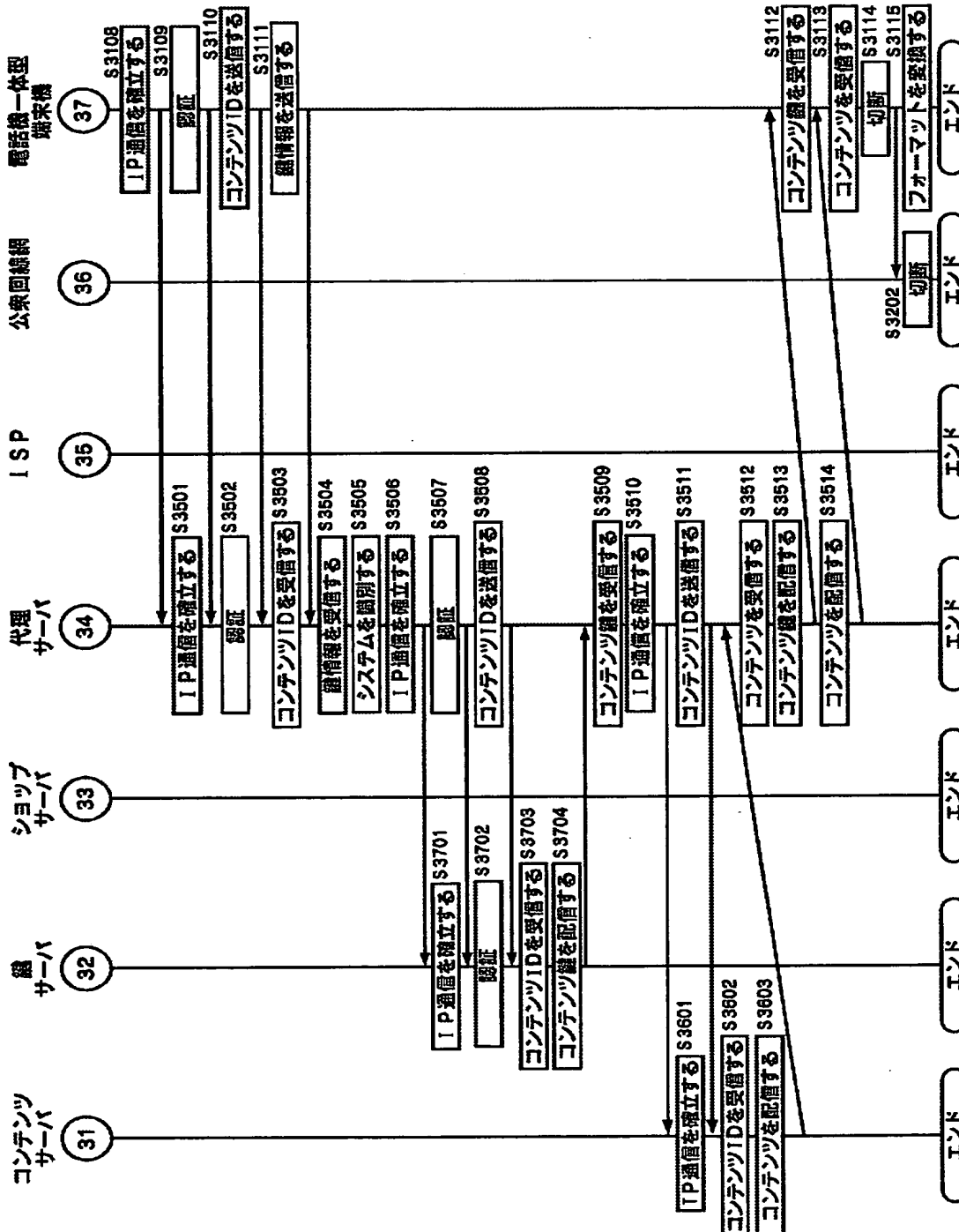
【図 13】

(13-1)

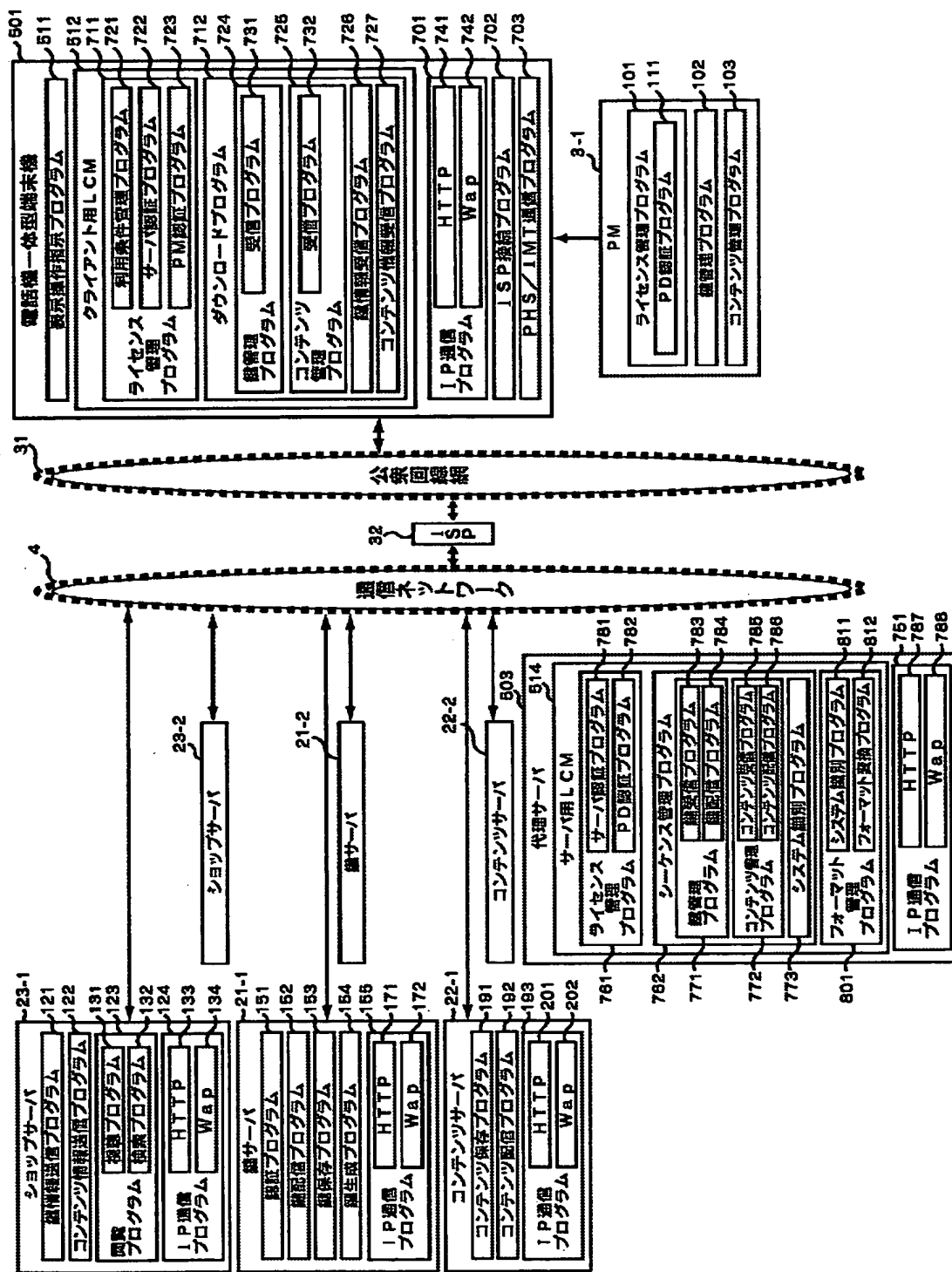


【図 14】

(13-2)

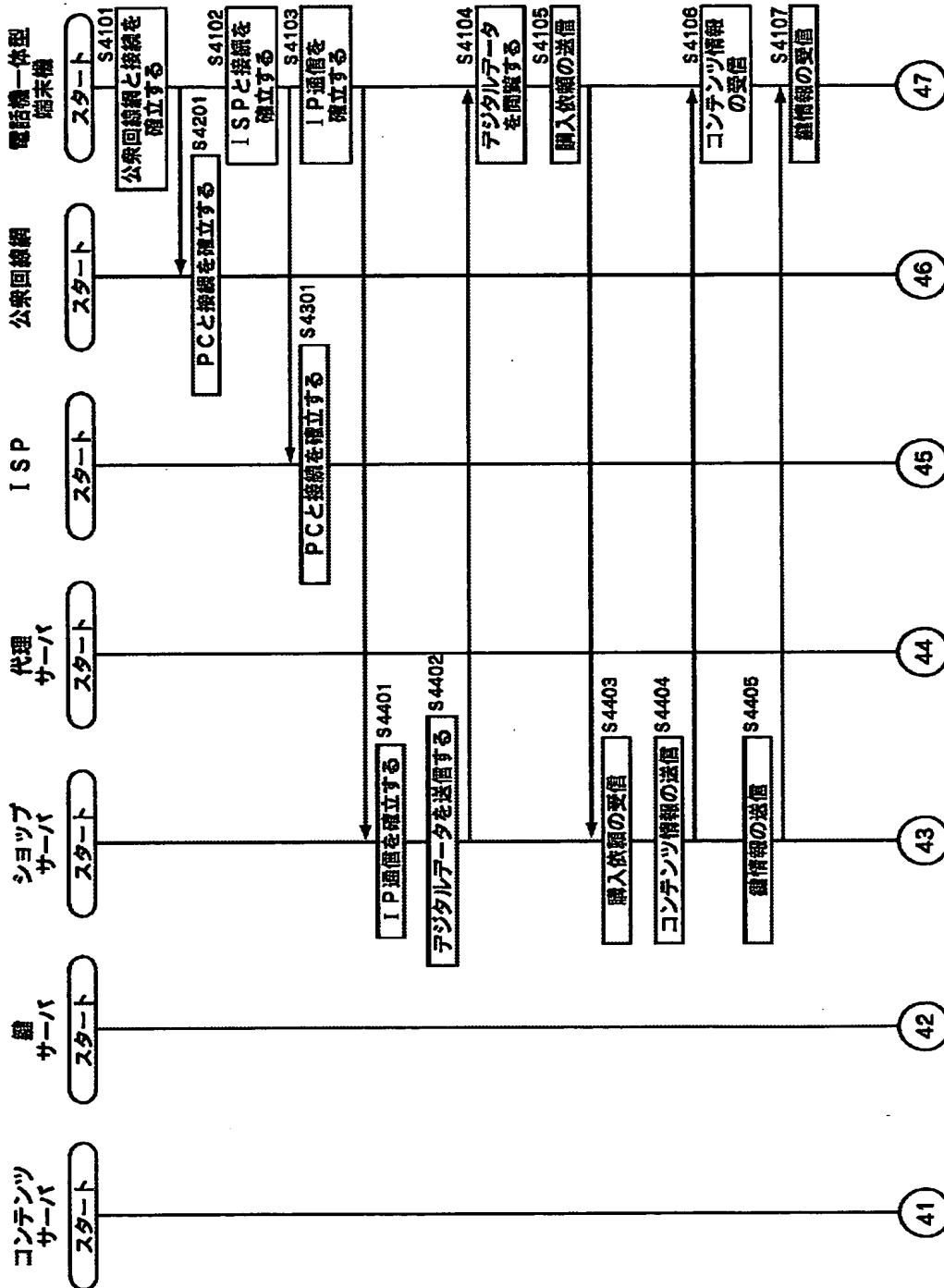


【图 15】



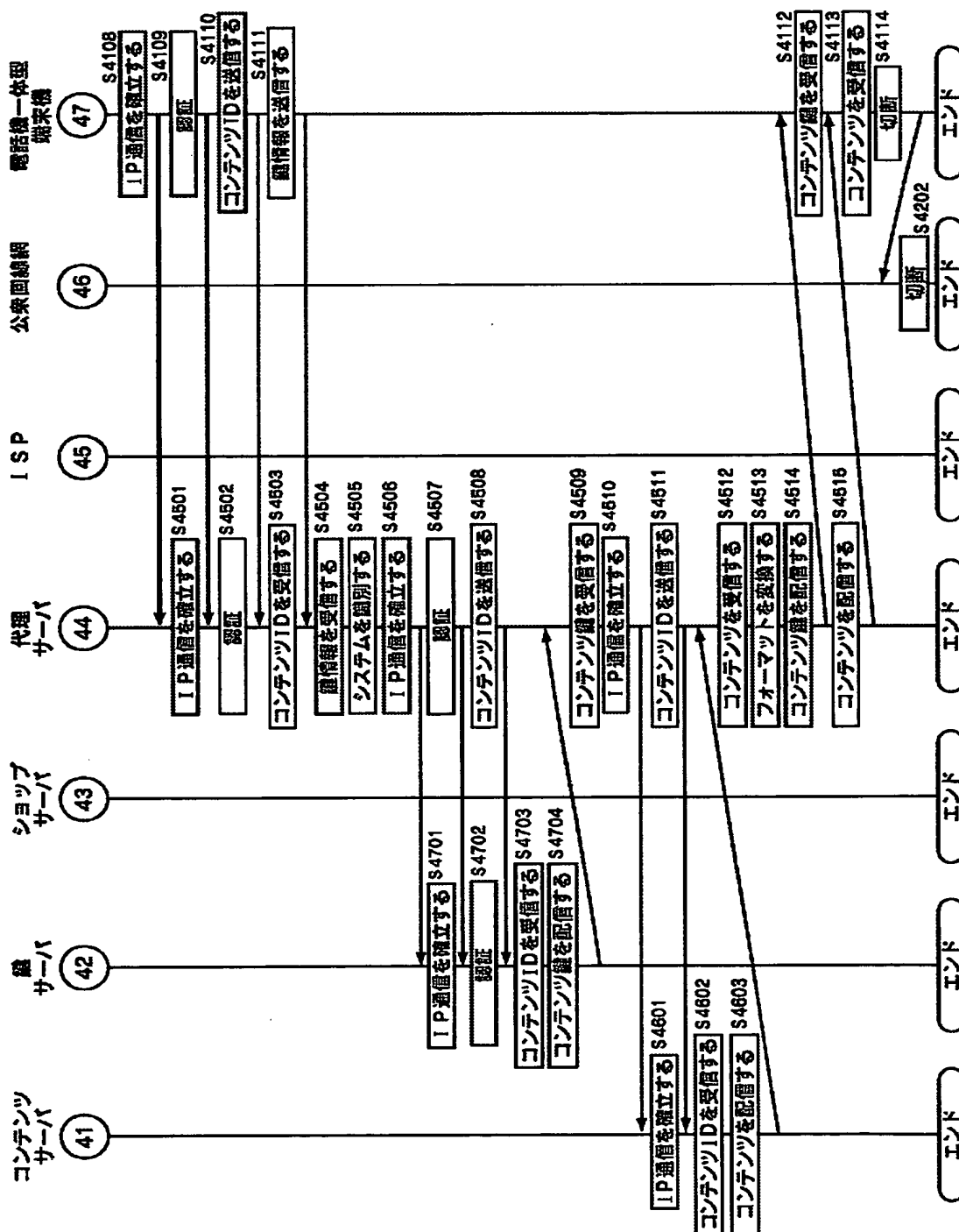
【図 16】

(16-1)



【图 1 7】

(16-2)



【書類名】 要約書

【要約】

【課題】 異なる手順で供給されるコンテンツおよび鍵を受信する。

【解決手段】 ライセンス管理プログラム 7 6 1 は、電話機一体型端末機 5 0 1 を認証するとともに、第 1 のサーバまたは第 2 のサーバを認証する。サーバ用 LCM 5 1 4 は、コンテンツおよび鍵の送信要求、並びに第 1 のサーバを特定するデータまたは第 2 のサーバを特定するデータの受信を制御して、第 1 のサーバを特定するデータを受信した場合、第 1 のサーバに対応する手続で、第 1 のサーバからコンテンツおよび鍵を受信し、第 2 のサーバを特定するデータを受信した場合、第 2 のサーバに対応する手続で、第 2 のサーバからコンテンツおよび鍵を受信するように通信を制御する。サーバ用 LCM 5 1 4 は、電話機一体型端末機 5 0 1 へのコンテンツおよび鍵の送信を制御する。

【選択図】 図 1 0



出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社